university of groningen

University Medical Center Groningen

University of Groningen

Privacy, free expression and transparency

Cannataci, Joseph A.; Zhao, Bo; Torres Vives, Gemma; Monteleone, Shara; Mifsud Bonnici, Jeanne; Moyakine, Evgeni

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2016

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):
Cannataci, J. A., Zhao, B., Torres Vives, G., Monteleone, S., Mifsud Bonnici, J., & Moyakine, E. (2016). *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*. (UNESCO Series on Internet Freedom). United Nations Educational, Scientific and Cultural Organization.

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license. More information can be found on the University of Groningen website: https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment.

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Download date: 05-05-2023

UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

Privacy, free expression and transparency

Redefining their new boundaries in the digital age

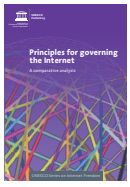
Privacy, free expression and transparency

UNESCO Series on Internet Freedom

UNESCO Series on Internet Freedom

UNESCO has started in 2009 to commission this flagship series publications of Internet Freedom, aiming to explore the changing legal and policy issues of Internet and provide its Member States and other stakeholders with policy recommendations aiming to foster a conducive environment to freedom of expression on the net.

This is the 7th edition of the series, with previous editions presented as below:



Principles for governing the Internet

As the sixth edition in the UNESCO Internet Freedom series, this study encompasses both quantitative and qualitative assessments of more than 50 declarations, guidelines, and frameworks. The issues contained in these documents are assessed in the context of UNESCO's interested areas such as access, freedom of expression, privacy, ethics, Priority Gender Equality, and Priority Africa, and sustainable development, etc.

Countering Online Hate Speech

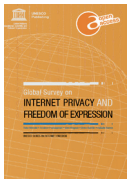
The study provides a global overview of the dynamics characterizing hate speech online and some of the measures that have been adopted to counteract and mitigate it, highlighting good practices that have emerged at the local and global levels. The publication offers a comprehensive analysis of the international, regional and national normative frameworks, with a particular emphasis on social and non-regulatory mechanisms that can help to counter the production, dissemination and impact of hateful messages online.

Building digital safety for journalism: A survey of selected issues

As technologies develop, so do opportunities as well as threats to journalism. This research explains some of the emerging threats to journalism safety in the digital era, and proposes a framework to help build digital safety for journalists. Examining 12 key digital threats to journalism, ranging from hacking of journalistic communications, through to denial-of service attacks on media websites, it assesses preventive, protective and pre-emptive measures to avoid them. It shows too that digital security for journalism encompasses, but also goes beyond, the technical dimension.

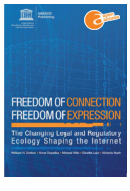
Fostering freedom online: the role of internet intermediaries

With the rise of Internet intermediaries that play a mediating role between authors of content and audiences on the internet, this UNESCO publication provides in-depth case studies and analysis on how internet intermediaries impact on freedom of expression and associated fundamental rights such as privacy. It also offers policy recommendations on how intermediaries and states can improve respect for internet users' right to freedom of expression.



Global survey on internet privacy and freedom of expression

This publication seeks to identify the relationship between freedom of expression and Internet privacy, assessing where they support or compete with each other in different circumstances. The book maps out the issues in the current regulatory landscape of Internet privacy from the viewpoint of freedom of expression. It provides an overview of legal protection, self-regulatory guidelines, normative challenges, and case studies relating to the topic. .



Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet

This report provides a new perspective on the social and political dynamics behind the threats to expression. It develops a conceptual framework on the 'ecology of freedom of expression' for discussing the broad context of policy and practice that should be taken into consideration in discussions of this issue.

All publications can be downloaded at:

http://www.unesco.org/new/internetstudy

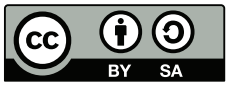
Joseph A. Cannataci
Bo Zhao
Gemma Torres Vives
Shara Monteleone
Jeanne Mifsud Bonnici
Evgeni Moyakine

Privacy, free expression and transparency

Redefining their new boundaries in the digital age

Published in 2016 by the United Nations Educational, Scientific and Cultural Organization,
7, place de Fontenoy, 75352 Paris 07 SP, France

© UNESCO 2016
ISBN 978-92-3-100188-8



This publication is available in Open Access under the Attribution-ShareAlike 3.0 IGO (CC-BY-SA 3.0 IGO) license (http://creativecommons.org/licenses/by-sa/3.0/igo/). By using the content of this publication, the users accept to be bound by the terms of use of the UNESCO Open Access Repository (http://www.unesco.org/open-access/terms-use-ccbysa-en).

The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The ideas and opinions expressed in this publication are those of the authors; they are not necessarily those of UNESCO and do not commit the Organization.

A research report
by STeP – Security, Technology and e-Privacy – Research Group
European and Economic Law Department,
Faculty of Law, University of Groningen
The Netherlands

This report was commissioned by UNESCO in January 2015, three months before the creation by the UN of the post of Special Rapporteur for Privacy and six months before the appointment of the lead author of this report, Prof. Joe Cannataci as the first UN Special Rapporteur for Privacy. For the avoidance of doubt, it is declared that the bulk of this report was completed before his appointment and that its findings and recommendation are completely independent from and do not represent the official views of the Mandate of the UN Special Rapporteur on Privacy.

Acknowledgements
The co-authors from STeP, Prof. Joseph A. Cannataci, Dr Bo Zhao, Ms Gemma Torres Vives, Dr Shara Monteleone, Prof. Jeanne Mifsud Bonnici and Dr Evgeni Moyakine, gratefully acknowledge the assistance of colleagues from the Department of Information Policy & Governance at the University of Malta, Dr Aitana Radu and Dr Christian Bonnici, for their review of and contributions to the final drafts of this report. The co-authors also acknowledge the contribution of a number of edits suggested by colleagues from UNESCO, especially Dr Xianhong Hu and other members of UNESCO Secretariat.

UNESCO thanks the support of the Ministry of Foreign Affairs of the Netherlands for delivering this publication.

Kingdom of the Netherlands

Cover illustration: © Shuttershock/greiss design

Typeset and printed by UNESCO
Printed in France

Table of contents

Foreword

It is widely agreed that human rights should apply as much online as offline, and that freedom of expression and privacy should be no exception. But there are particular complexities in the online environment.

This publication explores these issues in the context of UNESCO's new approach to Internet issues. The approach was adopted by our 195 Member States in November 2015, and is based on the Outcome Document of an earlier conference called CONNECTing the Dots.

Concretely, this means that UNESCO stands for the concept of "Internet Universality" and the related "ROAM principles" which refer to a Human-rights-based, Open and Accessible Internet that is governed by Multi-stakeholder participation.

It is in this context that the current study was commissioned to address very specific rights and associated values.

First is freedom of expression – which entails (a) the right to impart information (seen especially in the right to press freedom); (b) the right to seek and receive information (seen especially in the right of access to information, or "right to information").

Second, and linked in part to the right to information, is the value of transparency – which means the openness of relevant documents and processes to the public.

Third is the right to privacy – which refers to a protected sphere for development of the personality and control of personal information.

Questions immediately arise at the points of intersection of these three issues.

For example, does transparency exist in inevitable tension with the right to privacy?

And: Is privacy an intrinsic obstacle for people's right to seek and impart information, for instance through investigative journalism?

Traditionally, potential tensions between rights have been weighed on a case by case basis in terms of international human rights standards. These standards thus allow for the limitation of one right in the interests of other rights, as long as this is necessary, proportional, for legitimate purpose and set out in law. All this is in order to preserve the basic essence of the limited right, and to ensure that limits are exceptional and that freedom for the right is the norm.

In the digital age, the challenge is to see how tensions between rights operate in relation to the Internet, and therefore in relation to the ROAM principles.

To illustrate, we are faced with a challenge about issues online like privacy invasion, mass surveillance, filtering and blocking. When are these legitimate limits of rights, and when do they become violations of the same?

What about considerations of Openness, Accessibility, and Multi-stakeholderism?

The purpose of the current research was precisely to unpack some of these issues. In particular, it probes the complex interplay on the Internet between the right to freedom of expression (and information), transparency, and the right to privacy. The research explores the boundaries of these rights, and the various modalities of reconciling and aligning them.

The study analyses the legal framework, current mechanisms for balancing rights, and specific issues, cases and trends. As revealed by the research, traditional laws and regulations for the protection of privacy and freedom of expression often do not deal with digital issues.

Also covered are the interplay and interactions between multiple players—e.g. the State agents, Internet users, ICT companies, civil society organizations, the judiciary and the security services. Various policy recommendations are made that address both key issues and various stakeholders groups.

The study serves as a response to specific points in the CONNECTing-the-dots Outcome Document. One is option 6.3, which proposes that UNESCO "support Member States as requested in the harmonization of relevant domestic laws, policies and practices with international human rights law". The second is 6.4, which envisages: "Support transparency and public participation in the development and implementation of policies and practices amongst all actors in the information society".

We hope, therefore, that this research will contribute to the ongoing policy debates in our Member States and their societies about Internet freedom, and help to promote free expression, privacy and transparency in the global Internet eco-system.

UNESCO expresses its thanks to the authors of this publication: Prof. Joseph A. Cannataci, Dr Bo Zhao, Ms Gemma Torres Vives, Dr Shara Monteleone, Prof. Jeanne Mifsud Bonnici and Dr Evgeni Moyakine for having conducted this comprehensive and in-depth assessment. UNESCO also thanks those international experts: Mr Danilo Doneda, Mr Lyad Kallas, Mr Pedro Less Andrade, Mr Danny O'Brien and Ms Carolina Rossini who have kindly participated in the consultation workshop and contributed to the first draft at the 10th Internet Governance Forum held in Brazil in 2015.

Frank La Rue

Assistant Director
General of UNESCO

Executive summary

The proliferation of the Internet increasingly facilitates the connection and communication between individuals and the rest of the world. It has also been re-organizing aspects of human life in an unprecedented manner. The unique characteristics of the technology—e.g. connectivity, openness, resilience and speed—have propelled the Internet to a dual status technology that differs significantly from other interactive communications media (like the telephone) and passive recipient communication media (like radio and TV), making it both a principal *communicating medium* and *a distinctive* and *extended life sphere* that embraces a wide range of human activities and interactions, old or new. Within this context, it is often argued that the online virtual world is in some respects no less important than the traditional physical and analogical world.

How these in-depth changes have had or continue to have a critical impact on important human rights, such as the right to privacy and the right to freedom of expression, is still an open question. How these relate to transparency is yet another topic in need of further inquiry. One of the potential causes of the lack of definitive or clear answers is the constant advance and evolution in digital technology. While the Internet and related Information and Communication Technologies (ICTs) have created more opportunities for the extension and enhancement of these two fundamental rights, there is little doubt that the Internet is also generating more challenges, risks and threats to the same two rights, and to their interrelations with the notion of transparency.

In this Report we seek to explore these issues further to provide at least partial answers to these open questions. One of our findings in the emerging *Internet Eco-system,* is the right to privacy in an online context which primarily refers to the right of individuals to information/data privacy, which is subject to increasing threats that come from multiple sources and in various forms. For instance, increases in the use of Privacy-Invading Technologies (PITs) have contributed to a gradual collapse in the traditional *communal boundaries* established by such constructs as law, morals, communal rules, physical obstacles, technical limits, and geographical barriers, contributing to privacy invasions as reported across the globe. Given that the new virtual world and the emerging information economy are based on digitized data and cannot function without data collection and data processing, we must understand that the control of personal information and personal data is a critical element in the digital age, if we aspire to values such as the individual's dignity, autonomy and liberty.

The Internet and the underpinning ICTs have also enabled a wider range of individuals to access and share more information globally, and to make greater use of their right to freedom of expression. It has also, by enabling a more efficient communication between individuals, enlarged the scope of the right to freedom of expression and opinion, often promoting transparency as a notion that lies at the core of other public interests. However, the misuse of this fundamental right can also contribute to the violation of other rights. Examples of such violations can be witnessed all across the globe, in cases of online defamation, online harassment and stalking, explicit hate speech, incitement to ethnic, religious or racial hatred, and online terrorist activities that threaten public order and security. Thus it is widely accepted that there is a global need to respond to the abuse observed in online speech so as to achieve a balance with other conflicting fundamental values and public interests.

One of the main threats to the right to privacy and the right to freedom of expression is the mass surveillance conducted by some nations over both foreign citizens and their own nationals. Recent spectacular revelations point towards the magnitude to which State actors could exploit contemporarily available technologies for multiple purposes, which erode the two rights, as well as other principles of the rule of law and democracy. It has also become clear that private actors, particularly large companies providing online services relating to search engine functionality, social networking and e-commerce, have adopted a business model that often depends heavily on the exploitation of personal data in ways that are not transparent, or in ways not immediately apparent to the users. Similarly worrying is the fast adoption and deployment of new ICTs by a number of States to monitor, censor and control political dissent.

An additional aspect to consider is the interplay between the right to privacy and the right to freedom of expression (including other corollary rights) in the digital age, when the boundaries between the two rights need to be re-defined to accommodate in stances of collision. For example: how do we redefine the balance between a public figure's right to privacy and the rights to freedom of expression as exercised by media and journalists? Given the rapid evolutions enabled by the Internet, what constitutes a public figure or a journalist? How does the notion of transparency link to the interplays between the rights of freedom of expression and privacy?

This Report, approaching the issues described above from an individual citizen's perspective and based upon research findings emerging from multiple sources, also strongly recommends that further actions be taken in the following aspects in order to tackle the challenges and threats linked to the two critical human rights under discussion. A number of concrete recommendations are presented in more detail in Chapter 9.

This Report follows UNESCO's new approach to Internet issues, as endorsed in November 2015 on the occasion of its 38th General Conference. At that meeting, the Organisation's 195 Member States adopted the Outcome Document of the UNESCO-convened multi-stakeholder conference called CONNECTing the Dots. In this document, 38 options for future action from UNESCO are set out; as well as the Internet Universality principles (R.O.A.M.), which advocate for a Human-rights-based, Open and Accessible Internet, governed by Multi-stakeholder participation.

CHAPTER 1 Introduction

The Internet has re-shaped human life and human society by providing both a significantly novel and influential communication medium, and an extended but distinctive virtual sphere that embraces a wide range of human activities. Yet, there is still the pending issue of how the Internet and the underpinning Information and Communication Technologies (ICTs) are influencing the realization of the human rights of privacy and freedom of expression, and the social value of transparency.

In this Report we seek to provide some partial answers to these open questions, by describing the ongoing challenges and threats faced by these two critical rights and the social value of transparency, and their interplay in the context of the advances in digital technology. The research was conducted on the basis of the following two main assumptions: a) since the advent of the Internet we have witnessed the development of new Internet eco-systems with special characteristics that may require a different legal treatment; and b) one of the fundamental issues that results from the novel digital ICTs developed in the past decades is the gradual collapse or blending of boundaries in human communities.

The authors of this Report believe that the Internet could now be evolving from a network of identical/similar networks, as originally intended by its creators, into something more; i.e. a large eco-system composed of smaller eco-systems. From a technical perspective, while the communication protocols enabling the Internet—i.e. the Transmission Control Protocol (TCP) and the Internet Protocol (IP), normally referred to collectively as 'TCP/IP'—were designed to enable the routing of data packets within and across historically very similar and quasi-identical computer networks, we now witness the emergence of new patterns, with some of the computer networks that form the Internet differing significantly from other such networks, while also leaving room for the continued growth of these divergences. Indeed, IPv6 differs significantly from its precedent, IPv4, enabling IPv6-enabled systems to form an eco-system that will be significantly distinct from the IPv4-dominated Internet that we know today, at least at the Open Systems Interconnection (OSI) layer.

From a less technical perspective, it is possible that we are also witnessing the creation of different spaces inside the Internet segregated either by existing national boundaries or virtual spaces dictated by technical and/or contractual means. In the first case, a country may use existing technology to define an Internet space that corresponds with its geographical borders using a variety of methods to control inward, outward and intra-border traffic flows. Given that such controls may differ from those exerted by other countries, they may, apart from creating partially distinct Internet spaces that nonetheless permit inward and outward communications from and to other such spaces, enable the existence of different Internet-based experiences.

On the other hand, local, regional and international organisations may use innovative technologies to create separate Internet spaces and rules that would, possibly, be subject to separate or specified jurisdictions that may differ from the jurisdiction of the country in which the Internet user resides. By using technical means such as, for example, an overlay of software,[1] such organisations may conceivably create a part of cyberspace using different protocols superimposed over the current TCP/IP protocols which could be open to anybody

1 See, for example, Christian Grothoff, Martin Schanzenbach and Matthias Wachs, "A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System", in Dimitris Gritzalis, Aggelos Kiayias and Ioannis Askoxylakis (Eds.), (2014) *Cryptology and Network Security*, Lecture Notes in Computer Science 8813, Cham: Springer International Publishing, available at <http://grothoff.org/christian/gns2014wachs.pdf>.

in most countries, allowing access to such virtual spaces. Legal means may also be used to compel users to observe different defined spaces on the Internet. The rules of behaviour, sanctions and governance inside such virtual spaces could differ from those that exist outside the spaces, in much the same way that the rules of behaviour in some countries could differ from those of others.

No value judgement is being implied here. Countries may choose to adopt a national approach. They may choose to adopt or create a virtual space that constitutes a common jurisdiction. The key issue is whether on balance, the consequence is on one hand Internet Universality with its associated benefits which include various diversities, or on the other hand, fragmentations into divided and isolated zones which inhibit the exclusion of knowledge societies around the world and the achievement of global sustainable development objectives.

How international human rights standards would apply to a fragmented scenario remains a matter for debate, relating to multiple layers of connected networks with numerous sources of rules and norms of different cultural and political origins. However, one widespread characteristic in this evolving Internet eco-system is the collapsing of boundaries historically ingrained in human life due to the rapid advances in digital technology. The nature of previous privacy boundaries is influenced by new Privacy Invading Technologies (PITs), such as body scanners; speech identification mechanisms; radio frequency identification (RFID) chips, which may also be human implantable; Closed-Circuit Television (CCTV); smart meters; canvass finger printing; and browser cookies, which are capable of enabling the collection of personal data from multiple locations. As pointed out by scholars, even the most secured home nowadays cannot protect from privacy invasion, in a variety of manners.[2]

Within technical and commercial environments that involve functionalities that rely upon the collection, storage and/or processing of data, which often present constant threats to privacy, it is not difficult to abuse and misuse personal data for purposes not desired and/or consented to by the relevant data subjects. The principal form of privacy that is breached in such contexts is often referred to as 'information privacy'. This is, in part, because despite the dependence of such a world on the collection, storage and processing of all sorts of personal data, pre-digital privacy-protection mechanisms do not, in many aspects, transfer to the digitized virtual world.

Freedom of expression—including freedom *to* impart information and freedom *to* seek and receive information—is transitioning to a new era in which everyone who is connected to the Internet can, amongst other things: a) express themselves to others at a relatively low cost, and b) access information from all connected networks. In the Web 2.0 era, the Internet has become a new public sphere and forum that enables the imparting of, as well as easy access to, an unprecedented range of information, despite geographical boundaries. However, the ability to disseminate information on the Internet, coupled with free access to such information, including information on others, can harm other people's privacy, reputation and other rights in unprecedented ways. One telling example can be found in the numerous online privacy invasion and defamation actions across the world brought to courts by public figures, consequent to the enlarged volume and audience of online publication. Therefore, it is also the case that the laws and morals defining the

2 See, for instance Bert-Jaap Koops, "On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy", (2014) *Politica e Società*, No. 2.

fine boundaries between the scope of the right to freedom of expression regarding others and the protection of one's private life, are undergoing a process of delineation and shift in different human communities, while being widely recognised as both an unavoidable social reality and an open question.

What this Report therefore covers are the complexities of both free expression and privacy rights and of their inter-relation which may be mutually supportive in some instances and characterised by tension in others. Within this context, this Report carries out a discussion from the point of view of a global citizen in abstract, seeing beyond political, cultural and economic diversities in different human communities. It also attempts to focus on the common human online activities and human needs and sensibilities in the digital age, at a point in which a large part of human life has already been shifting into the online virtual world. In doing so, the Report follows a thematic problem-solution approach, first describing the existing problems relating to individual citizens, and subsequently pursuing potential solutions under available legal-technical frameworks.

The research findings of this Report are drawn from multiple sources, including United Nations Educational, Scientific and Cultural Organization's (UNESCO) previous research on online freedom of expression and privacy; reports from international NGOs and human rights organizations; commercial reports; a series of EU-funded research projects; scholarly works; UN special reports on the two rights; and outputs from multiple international and regional conferences regarding Internet governance. However, the Report is not a mere description of the status quo in the online world. Rather, it offers overarching reflections on the notions of online privacy, online freedom of expression, online transparency, and their interplay, with a focus on those aspects that did not exist in the pre-digital era.

We define the Internet as a computer network of connected computer networks, including artefacts and constructs at all levels, such as at the hardware level; software-level protocols and applications such as email, FTP and the Web; and content.[3] Privacy is a complex term that refers to a variety of notions within and across different cultures and communities, ranging from the right to be left alone, to physical solitude, to bodily privacy, to information(al) privacy and information self-determination, to shaming, to dignity and personality, to appropriation of likeness and name, to secrecy, etc. However, in the online world, and therefore also for this Report, the focus is generally on what is widely referred to as 'information privacy', which is closely related to other dimensions and meanings of the generic notion of privacy. Note that while in this Report we use the terms 'data privacy' and 'information privacy' interchangeably, these may sometimes differ from each other in concrete contexts.

Regarding freedom of expression (and opinion), we follow the traditional definition provided by the International Convention on Civil and Political Rights (ICCPR). Thus, we include freedom of expression and opinion, freedom of information and other corollary concepts—such as the notions of access to information and freedom of peaceful assembly—all of which fit into the online environment. Transparency is defined in this Report as an overarching concept and value that is a desired result that emerges from the exercising of the right to freedom of expression and information and enables enhanced free flows of information and thereby contributes to social goods like better governance, accountability and efficiency. These concepts are defined in detail in Chapters 3, 4 and 5.

---

3 See Footnote one in Jovan Kurbalija, (2014) *An Introduction to Internet Governance*, Sixth Edition, Msida and Geneva: DiploFoundation, available at <http://www.diplomacy.edu/resources/books/introduction-Internet-governance>.

The remaining part of this Report is organised as follows. Chapter 2 describes opportunities, threats and challenges of/from the Internet to the rights of information privacy and freedom of expression, as well as transparency at the individual, national and international levels. Chapters 3, 4 and 5 illustrate the related conceptions in law and outline the legal and alternative protection mechanisms linked to the three at the international, regional and national levels, explaining general legitimate limitations and restrictions. Chapter 6 explains aspects of the interplays between privacy, freedom of expression and transparency in different contexts, illustrating their mutual-independence and potential conflicts in daily life realities. It also describes how the two rights and the value of transparency have been balanced in some legal systems and the important and well-recognized international human rights standards to reach a reconciled relationship.

Chapter 7 then goes on to discuss what may be missing in the present rights protection mechanisms. It illustrates the increasing risks and threats to these rights due to the fast advances of new digital technologies and the increasing use of multiple portable devices in daily life. In particular, it debates the balancing of the rights to freedom of expression and privacy in three concrete circumstances: the Google Spain case, the privacy protection of public figures, and anti-terrorism legislation. Chapter 8 offers a brief review of the policies across the world in bridging the aforementioned gaps in these major aspects. Finally, the Report is concluded by Chapter 9, in which concrete policy recommendations are provided to improve the protection of individual information privacy and freedom of expression, as well as transparency in the digital age.

The present research was commissioned as part of the elaboration of UNESCO's Internet Universality framework, and particularly how to balance Rights against each other and in the light of Openness, Accessibility and Multi-stakeholder Participation, as per the RO.A.M, model. Specifically, it further responds to the options recommended by the CONNECTing the Dots Outcome Document that UNESCO "support Member States as requested in the harmonization of relevant domestic laws, policies and practices with international human rights law" and also "Support transparency and public participation in the development and implementation of policies and practices amongst all actors in the information society".

CHAPTER 2 The opportunities and threats from the Internet

Technology advances have responded to existing opportunities and created new opportunities, vastly expanding human capacities through increases in the volume of data, information, communication and knowledge, as well as through increases in the speed of the transfer of data, leading to human progress and enormous benefits. We should not lose sight of these opportunities and benefits, by overemphasizing the challenges and threats brought about by the same changes. Thus, the rational approach to the risk posed by the new technologies would involve careful consideration of both aspects of the coin. Such approach would aim to avoid, eliminate, mitigate or transfer the risks and enhance and expand the range of benefits, thus solving existing issues, devising conscious trade-offs and shaping the whole in the interest of humanity at large. Within this context, this Chapter assesses the issues as they impact on privacy, freedom of expression and transparency.

2.1 The death of privacy in the digital age?

The "death of privacy" in the 21st century was first predicted 15 years ago, inspired by accelerations in the development of technology.[4] Though the claim seems a bit exaggerated, the reasons underlying the conclusion drawn at that moment in time are still valid today in their capturing of the wide-ranging and frightening threats to individual privacy.[5] Most threats foreseen by the technical community have not failed the prediction. Rather, their presence has intensified by more advanced and unpredicted technologies. Similarly, the predominating threats to individual privacy in the past decade have gradually shifted from the offline, physical world to an online, virtual world, and the centre of privacy protection has accordingly moved from *physical* to *informational* privacy,[6] in the context of digitization and connectivity. Such threats to privacy, like the corresponding benefits, can be witnessed at different levels, including the individual, societal, national, and international levels.

At individual level

Information about normal daily events and human activities, whether we are travelling, buying, walking, sitting, sleeping, reading or talking, is increasingly captured and stored in digital form for later access and analysis. Indeed, we are witnessing drastic increases in the number and use of all sorts of sensing devices that contribute to the systematic monitoring of human living spaces, both public and private, including CCTV and video cameras, microphones, thermal sensors, surveillance satellites, drones, smart electricity meters, smart TVs, wearable devices and built-in RFID chips. Similarly, we witness the proliferation of biometric technologies including those involving the collection, storage and processing of genetic sequence data, and of the data involved in fingerprint-, facial-, iris-, speech- and gait-recognition used for the identification of human beings for different purposes.

---

4 See among others Simson Garfinkel, (2001) *Database Nation: The Death of Privacy in the 21st Century*, Sebastopol: O'Reilly Media.

5 Ibid., pp. 10-12.

6 Physical privacy refers to the restricted access of others to our bodies, relationships and living spaces. See Keith Bauer, "Healthcare Ethics in the Information Age", in Rocci Luppicini and Rebecca Adell, (2008) *Handbook of Research on Technoethics*, Hershey: Information Science Reference an imprint of IGI Global, p. 179. Information privacy refers to "the handling of 'personal information', that is, information about a particular person or information that can be used to identify a particular person". See Australian Privacy Commissioner, "What Is Information Privacy and Why Do We Need to Protect It?", August 1997, available at <http://www2.austlii.edu.au/itlaw/national_scheme/national-PART.html>. Information privacy and other related conceptions will be discussed further in Chapter 3.

On the one hand, the data-ization of life can protect aspects of private lives, such as religious, political and sexual orientation, which formerly could only be expressed in a relatively public manner and which individuals often had to suppress. On the other hand, it may enable new intrusions and exposures. For example, it would appear from the widespread on-going debates that the human community, as a whole, still lacks the wisdom or ability to handle data fairly and justly, especially in terms of what should or should not be generated, stored and used. As a result, such data is often subject to intentional or accidental information security breaches and can subsequently be accessed and interpreted by anyone capable of doing so, while at times also rendered available to others, including the general public. The effects of such breaches may also be exacerbated by rapid advances in data processing technologies, including in those enabling automatic and big data processing. As an additional example, information privacy breaches may contribute to physical privacy breaches—which refers to the unwanted access to human bodies and living spaces—such as when burglars are equipped with hacked personal data revealing the absence of occupants of a premise and/or the layout of the space and its infrastructure.

In the digital age, individuals become increasingly vulnerable to privacy invasions as they depend more on the use of the Internet to carry out their daily activities and thus they disclose more of their personal data to others. The risk comes from both the fact that personal data becomes progressively digitized and as a result of it being stored in several devices and locations. For instance, the personal data stored in a smartphone contains, in the eyes of the U.S.A. Supreme Court *'…a broad array of private information never found in a home in any form—unless the phone is [there]…'* The Supreme Court goes on to state that smartphones are *'…in fact minicomputers that also happen to have the capacity to be used as a telephone…'* and that such computer systems *'…can be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers…..'*[7]

Mounting online threats include hacking, identity theft, fraud, phishing, pharming, spoofing, profiling, spyware, tracking cookies, online witch hunting, bullying and stalking, which may involve a wide range of actions, including the unwanted disclosure of a user's personal information (sometimes known as "doxing"). This can be achieved either through the subject's intentional or unintentional online activities and/or through others' uploading of the subject's digital information acquired offline—such as video images or sound tracks—in the absence of the subject's consent and/or outside the data subject's immediate control. Such privacy-invading actions can cause data subjects a wide variety of damages, including the prompting of suicidal thoughts or actions due to the victim's loss of critical elements of human life, such as safety, personal identity, autonomy and dignity. These examples are evidence of how traditional boundaries between the public and the private, between the physical and the virtual, and between the past and the present are collapsing.

The challenges for ordinary individuals lie, mainly, in the technical complexity of online privacy breaches, which might only be well understood by a small group of well-educated elites, insofar as PITs are far beyond daily common knowledge. The popular 'I have nothing to hide' attitude often adopted by the users is another important factor contributing to weakened privacy[8]. Such an attitude reflects the increasing danger to personal data and the increasing value of privacy to personal development as an un-alienated human right, thus

7 United States Supreme Court, *Riley v. California 573 U.S.* (2014), paras. 21 and 17, available at <https://supreme.justia.com/cases/federal/us/573/13-132/>, accessed 17 May 2015

8 See in general Daniel J. Solove, (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven and London: Yale University Press.

extending until the moment that an individual confronts tangible immediate monetary harms such as e-theft or data destruction. Another common factor contributing to the erosion of privacy, is the privacy-for-service exchange practice widely adopted amongst Internet users, who tend to trade privacy for service partially because they feel incapable of controlling their personal information online.[9] Ironically, while many Internet users are increasingly aware of the significance of their right to information privacy in online contexts, they are not willing to take action even after experiencing information security breaches.[10]

Individuals can also be privacy invaders when they master new ICTs to collect information from the Internet or to gain illegal access to private information. This can occur by using malware, spyware, as well as needlecams, smartphone apps, and other hacking devices and techniques.

As individuals replace traditional photo cameras with multipurpose electronic devices such as smartphones and tablets to record aspects of both their life and others', it has become increasingly possible to rapidly upload the images taken through such devices to online locations, such as Social Networking Services (SNS), and to share them with other known or unknown parties. This often happens without first requesting or obtaining the implicit or explicit consent of the parties involved as data subjects.

The rapid decline in the costs of new technologies enables individuals equipped with fairly cheap digital devices to pose a growing threat to other people's privacy. For example, the increasing affordability of CCTV systems has enabled the installation of such systems in an increasing number of private homes, serving safety and security purposes, but also enabling the invasion of multiple parties' legitimate privacy interests.[11] Similarly, the increasing affordability and popularity of the private use of unmanned aircraft systems, or drones, may enable the breach of several parties' physical and information privacy, such as by the collection of audio-visual data during fly-passes over others' properties.[12] Another form of privacy invasion is the unauthorized appropriation of likeness of individuals, or expression of consumer preference to friends for commercial benefits through public exposure of such content.

As Zittrain noted in 2008, the Internet "enables individuals in many cases to compromise privacy more thoroughly than government and commercial institutions traditionally targeted for scrutiny and regulation".[13]

The consequences of privacy invasions in the digital age can be serious and have no sufficient remedy. Some of these may include mental distress and emotional loss (e.g. due to online stalking and bullying), financial loss (e.g. resulting from instances of identity theft and fraud[14]), as well as twisted interpersonal relationships, and trust and intimacy issues.

---

9 This is reflected in the most recent Ponemon research report on privacy and security among European, U.S. and Japanese consumers. Ponemon Institute LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers*, Research Report, March 2015, available at <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rt_privacy_and_security_in_a_connected_life.pdf>.

10 Ibid., pp. 1-2.

11 ECJ, Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, Judgment, 11 December 2014.

12 For the capacity of drones for privacy threats, see Jonathan Olivito, "Beyond the Fourth Amendment: Limiting Drone Surveillance through the Constitutional Right to Informational Privacy", (2013) *Ohio State Law Journal*, Vol. 74, No. 4, pp. 673-678.

13 Jonathan L. Zittrain, (2008) *The Future of the Internet--And How to Stop It*,, New Haven and London: Yale University Press, p. 200.

14 Though one must also be careful to nuance privacy from security in many such instances

Additionally, since the extraction of partial information from the whole picture about an individual may dominate an audience's overall image about the individual, whether such information would be disclosed online or offline, privacy invasions that lead to partial disclosures may cause inappropriate judgements regarding the individual. This could potentially lead to the transformation of individuals from 'subjects' to 'objects with shame'.[15]

On many occasions privacy invasions are conducted sporadically by private individuals, for individual purposes such as personal revenge or economic benefit. In contrast, large-scale invasions of privacy, widely acknowledged at a global level, are conducted by private corporations and States. The latter type of privacy breaches—which is considered further in the remaining part of this section—also differs from the former insofar as it relates more to the collective than to the individual, adopts an institutional nature, and as a result is likely to trigger more negative consequences.

At corporate level

Private business corporations may nowadays risk becoming a major source of privacy invasion, in many ways and for various reasons. Firstly, private ICT companies can misuse personal data that they collect in their daily business for economic benefits, exploiting the increasing value of data as a currency of the information economy.[16] Secondly, the collection and processing of personal data are now key to some companies' business models, to the point that some models involve the collection of private information either as a core part of the business or as a means to enhance efficiency, convenience and quality of service.[17] It has been alleged by some that, in the age of Big Data, privacy erosion is in a sense the business model.[18] Thirdly, traditional business enterprises and other entities often do not implement adequate controls to protect their consumers' personal data from external threats—e.g. as emerging from external hackers—and internal vulnerabilities—e.g. as emerging from internal employees—especially when lacking necessary technical and financial means to safeguard customers' personal data. As a result, information security breaches are reported on a regular basis in relation to customer and citizen data held by corporations and States. For example, Shopacheck, a loan firm in the UK, lost sensitive financial information pertaining to 1.4 million customers after two back-up tapes went missing in 2012.[19] Fourthly, commercial entities holding personal data may invade the data subjects' privacy by the unauthorised sale of the data to other companies or actors. In relation to this, even if the data subjects would have authorised such sales, few proper legal safeguards—e.g. a legal requirement for the anonymization of data—may be provided as well as enforced, and this increases the danger of potential data privacy invasion.

15 Jeffrey Rosen, (2001) *The Unwanted Gaze: The Destruction of Privacy in America*, New York: Vintage Books USA, p. 115.

16 "Personal data is the currency of today's digital market". See Viviane Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age", Speech, 22 January 2012, available at <http://europa.eu/rapid/press-release_SPEECH-12-26_nl.htm>.

17 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 98, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

18 Molly Wood, "In the World of Big Data, Privacy Invasion Is the Business Model," *CNET*, 29 February 2012, available at <http://www.cnet.com/news/in-the-world-of-big-data-privacy-invasion-is-the-business-model/>, accessed 7 April 2015.

19 Clinton Manning, "Shopacheck Loses Data on 1.4 Million Customers", *Mirror*, available at <http://www.mirror.co.uk/money/city-news/shopacheck-loses-data-on-14-million-157430>, accessed 17 May 2015.

In these contexts, many privacy invasions occur when personal data are processed automatically without sufficient human intervention, potentially enabling data-profiling-based discriminatory treatment of the data subjects, in many cases without the subject's knowledge. Another example of information privacy invasion, with similarly serious consequences, is the misuse of medical records and data, leading to unfair treatment of patients and additional data breaches, especially when Binding Corporate Rules (BCRs) are used and data anonymity and pseudonymity do not provide sufficient anonymization due to increasing capabilities to de-anonymise data based on available information.[20]

Another example of potential invasion of privacy is the arbitrary cooperation of private companies with intelligence services across the globe, providing to the latter systematic access to large databases that contain personal data. In 2013 the UN Special Rapporteur for Freedom of Expression and Opinion criticized the compliance by companies with State requirements in the design of digital networks and communications infrastructures. Specifically, he criticized those that enable, support or do not counter illegitimate intrusions by State, developing and deploying new technologies and communications tools in specific ways and being complicit in developing technologies that enable mass or invasive surveillance in contravention of existing human rights standards.[21]

At State level

Notable privacy invasions are conducted either by Law Enforcement Agencies (LEAs) or by intelligence services in the name of national security and public order. In the digital age, State authorities across the globe have been equipped with the most recent IT technologies, enabling them to monitor and conduct surveillance over individual citizens in an unprecedented manner.[22] Such activities involve the use of a combination of techniques, such as data profiling, CCTV systems, malware, and all types of installed sensors, biometrics, data automatics, and big data analytics. Privacy can be legitimately limited for national security reasons but only when the criteria of legality, necessity and proportionality are fulfilled, as prescribed by the standards of the ICCPR. Unfortunately, in many cases these conditions are not met.

Furthermore, in the context of the expanding adoption of e-governance, State authorities may be one of the biggest data hosts and controllers, handling large amounts of personal data. However, such data are not always sufficiently secured against invasion. Additionally, the fact that States may have unfiltered authority to access all sorts of personal data places individual citizens in a very vulnerable position if, for instance, appropriate legal mechanisms are not implemented to protect citizens in the case of data profiling. Threats to citizens' privacy and dignity also come from the shift of governance from human interference to another model based more on data automation and computing aimed at improving

20 See in general "Data Protection in the EU: The Certainty of Uncertainty", *The Guardian*, 5 June 2013, available at <http://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous>, accessed 30 March 2015. Also see Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization», (2010) *UCLA Law Review,* Vol. 57, p. 1701.

21 Office of the United Nations High Commissioner for Human Rights (OHCHR), Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, UN Doc. A/HRC/23/40, pp. 19-20, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

22 See, for example, the report of such activities carried by GCHQ in the UK. Privacy International, "Privacy International Challenges GCHQ's Unlawful Hacking of Computers, Mobile Phones", 13 May 2014, available at <https://www.privacyinternational.org/?q=node/471>, accessed 30 May 2015.

governance efficiency. One of the problems is the predictive privacy harm. The threat is that without consent or even without knowing what is happening back stage, individuals are treated differently by State authority based on data profiling and behavioural assessment. [23]

In some cases, there is also a problem rooted in the collapse of the previously established boundaries between intelligence services and law enforcement activities, as there are insufficient legal baselines for how different functions relate to limits or privacy intrusions. As a result, particularly after the 9/11 attacks in the USA, urgent anti-terrorism needs are successfully employed as arguments to justify massive interceptions of private communications and online activities. Yet, mass surveillance is not only a big threat to the privacy and dignity of ordinary individuals,[24] but it can also become, in the long run, a potential source of weakness for State authorities themselves by diminishing trust and credibility.

Another issue to be considered is the inequality between local and foreign data subjects in a particular state. For instance, foreign data subjects are less protected by the USA's law than by the European data protection law which provides equal information privacy protection for local and foreign citizens. In the digital age, in which personal data can be collected, stored and processed anywhere, mostly across borders, protecting information privacy in cross-border data processing is a major challenge. This is of particular importance in view of the escalating conflicts of jurisdiction and laws, and in view of the few legal remedies available for data privacy invasion on foreign territory. Although right now this concerns mostly citizens of developed countries, it will become a major legal problem for the international society to tackle.

At the international level

Due to the openness and connectivity of the Internet, some threats to individual privacy emerge from cross-nation online privacy breaches and invasions orchestrated by cyber criminals, such as cross-border online frauds, phishing, stalking and harassment, as regularly reported for causing a wide range of losses, including individual monetary losses and the loss of human lives.[25]

The picture becomes even more complicated when national interests are involved, whether these are of a military, political or economic nature. In addition to conflicts of laws and jurisdictions relating to the increasing cross-border data transfers, significant challenges emerge from the widespread practices of State espionage and large scale data breaches that are supposedly conducted by national States enjoying technology advantages. For example, the breach of Sony Pictures Entertainment entailed the online publication of documents containing personal information about Sony's employees.[26] Another example is the unauthorised access of around 80 million records stored at Anthem Inc., the second

23 See in general Kate Crawford and Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", (2014) *Boston College Law Review*, Vol. 55, No. 1, p. 93.

24 In the sense that it violates the moral-legal principle of presumption of innocence. See Jonida Milaj and Jeanne P. Mifsud Bonnici, "Unwitting Subjects of Surveillance and the Presumption of Innocence", (2014) *Computer Law & Security Review*, Vol. 30, No. 4, pp. 419-428.

25 See "Man Charged in Netherlands in Amanda Todd Suicide Case", *BBC News*, accessed 8 May 2015, available at <http://www.bbc.com/news/world-europe-27076991>.

26 Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far", *WIRED*, 3 December 2014, available at <http://www.wired.com/2014/12/sony-hack-what-we-know/>.

largest US health insurer.[27] In this context, privacy protection is related to data security which falls within the public security responsibilities of the State, but there are complexities when the breached infrastructure is private rather than public.

2.2 Freedom of expression online: enlarged but endangered

Freedom of expression has been widely recognized both as a fundamental human right and as a pre-condition for open and democratic societies.[28] It is also well-accepted that the exercising of this right has changed and improved in many ways over the past decades, especially by the connection of so many individuals to an online space, characterized by unprecedented openness, decentralization, connectivity and equality. Nowadays, individual citizens with basic access to the Internet and minimum knowledge of their IT devices and the software/apps running on such devices, can transform themselves from passive readers to online content generators, thus gaining more speech power than ever before.[29] These online activities enable people not only to seamlessly express themselves and communicate with others, but also to instantly reach huge audiences.

Freedom of expression is enlarged in the digital age not only by extending its access dimension, but also by enabling innovative ways to communicate and diffuse information. The online dissemination of information and opinions bears fewer limitations relating to space or geographical boundaries, no limitations relating to time or formats, and generates participant roles characterized by interactivity[30].

Multiple online communication instruments and channels have also facilitated online assembly and association activities. Nowadays, anyone having access to the Internet can associate or assemble with others in cyberspace, oftentimes more easily than is possible physically. This functionality enables the achievement of common goals and the attraction of public attention, including via online video chats, online meetings, and SNS-based social groups. Indeed, as showcased during the political transformations and unrest in parts of the Arab world , the right to 'free assembly and association'—as the cross-pollinating sister of the right to freedom of expression, including in online contexts—plays an important contributing role in the democratisation process.[31] The same right is also considered *'… essential for people's participation in the public debate and their exercise of democratic citizenship…'*.[32]

SNSs can play a particularly important role in virtual assembly and association, enabling individuals to both accentuate their voice and mobilize others. This right has been emphasized as one of the Internet Governance principles at NETmundial, the Global Multistakeholder Meeting on the Future of Internet Governance at Sao Paulo, Brazil in 2014: *'…Everyone has the right to peaceful assembly and association online, including through social*

27 Karen Freifeld, "U.S. States Probe Massive Data Breach at Health Insurer Anthem", *Reuters*, 6 February 2015, available at <http://www.reuters.com/article/2015/02/06/us-anthem-cybersecurity-probe-idUSKBN0L92NP20150206>.

28 UNESCO, Internet, Privacy and Freedom of Expression, p. 10.

29 See Hans-Juergen Bucher, "The Power Of The Audience: Interculturality, Interactivity and Trust in Internet Communication: Research Design and Empirical Results", (2005) *The Electronic Journal of Communication*, Vol. 15, Nos. 1-2, available at <http://www.cios.org/EJCPUBLIC/015/1/01511.HTML>..

30 For the previous four lack of limitations, see Ibid., pp. 6-8.

31 Wolfgang Benedek and Matthias C. Kettemann, (2014) *Freedom of Expression and the Internet*, Council of Europe, p. 38.

32 David J. Harris et al., (2009) *Law of the European Convention on Human Rights*, Second Edition, 2009, Oxford: Oxford University Press, Notes 17 and 1.

networks and platforms…' [33] Nonetheless, the notion of freedom of expression, though enlarged and complemented by the Internet, has also encountered new risks. The blurring of the traditional socio-legal boundaries, as in regard to privacy, leads to challenges to both other human rights and freedom of expression itself in the evolving Internet eco-system.[34]

For instance, the misuse of the right to freedom of expression in online contexts can cause considerable damage to other individuals' rights, such as those to privacy, reputation and dignity and other public interests, such as public security and public order. As an example, terrorist and religious extremist groups have been using such SNSs as Facebook and Twitter to advocate ideologies, recruit new believers and mobilize activities that have caused substantial harm.[35] Similarly, hate speech, gender and racial discrimination speech, and Holocaust denial expressions may offend widely-held public values and potentially incite violence, discrimination and hostility. Likewise, freedom of speech online can be abused if sensitive personal information is disclosed without the subject's consent or in the absence of a public interest-based justification. This can lead to invasions of individual privacy, and the compromise of the subject's dignity, autonomy, reputation and social relationships.

Some well-known, albeit extreme instances of such abuses of the right to freedom of speech in online contexts, involve criminal activities like online stalking and witch-hunting, which have at times been serious enough to contribute to, or even cause, the loss of human lives. Other instances of such abuses of the right to freedom of expression online could encourage the circulation of rumours and false information, leading to the polarization of individuals and groups,[36] which in recent years may have contributed to the compromise of trust amongst Internet users, and of the Internet itself.[37] While such problems are not alien to the pre-digital age, they have indeed multiplied and amplified in the digital world.[38]

Access to information is also a complex issue. As the Internet becomes a world forum involving all its users, and a world archive that stores each piece of information uploaded, powered by increasing decentralization and technology developments in data storage, it poses new and special risks and challenges.[39] For instance, a challenge to human society relates to the notions of 'data persistence' and 'data retention' – the idea that the Internet never forgets.[40] While a human being has a moral right to grow and develop by learning from past mistakes, and therefore deserves a second chance to start over from the past, the Internet provides a social environment that may inhibit or deny such a chance. Indeed,

---

33 NETmundial, "NETmundial Multistakeholder Statement", 24 April 2014, p. 3, available at <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

34 See introduction and discussion of the new eco-system in Chapter 1.

35 United Nations Office on Drugs and Crime (UNODC), *The Use of the Internet for Terrorist Purposes*, Report, September 2012, Vienna: United Nations, available at <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>..

36 See in general Cass R. Sunstein, (2009) *On Rumors: How Falsehoods Spread, Why We Believe Them, What Can Be Done*, New York: Farrar, Straus and Giroux.

37 See a discussion by Bucher in Hans-Juergen Bucher, "The Power of The Audience: Interculturality, Interactivity and Trust in Internet Communication: Research Design and Empirical Results", (2005) *The Electronic Journal of Communication*, Vol. 15, Nos. 1-2, available at <http://www.cios.org/EJCPUBLIC/015/1/01511.HTML>.

38 UNESCO, Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, Report, 2015, Paris: UNESCO, p. 36, available at <http://unesdoc.unesco.org/images/0023/002325/232563E.pdf>.

39 In view of the copy-and-paste works done by individual Internet users and the bulk of data collected automatically online by web crawlers by different digital institutions including for example Google and the Internet Archive.

40 See in general Viktor Mayer-Schönberger, (2011) *Delete: The Virtue of Forgetting in the Digital Age*, New York: Princeton University Press.

digital footprints—i.e. the traces or «footprints» that people leave online over time—may lead or encourage spectators to blend a person's past with the present, missing out on substantial changes and discontinuities[41], pass ill judgement about the subject, and/or stifle individual development. This is the stated reason why the European Court of Justice (ECJ) has decided in the Google Spain case to limit access to the litigant's past information on the Internet.[42] Nonetheless, the scope of "the right to be forgotten" is debatable.[43]

A no less important issue regarding freedom of expression in online contexts, with a specific focus on political expression, is what is widely referred to as the 'digital divide'. Generally speaking, people of higher social-economic status can represent themselves with the power of digital means, and as a result often gain more support from others who would share similar opinions. Weak opportunities for accessing digital means will hinder a certain part of human community from accessing information, and from expressing their voices and ideas to others. On similar lines, digital illiteracy—which refers to a person's inability to perform tasks effectively in a digital environment—renders it impossible for many global citizens, especially those coming from developing countries, to take up the opportunities presented by the Internet to more effectively participate in politics and public issues.

In some communities the problem with the digital divide has been taken to another level, which is characterized by differentiated Internet use.[44] For instance, empirical research has shown that in the Netherlands, some people use the Internet to gain access to more information than others who seem to engage more in social interaction and gaming, which are both very time-consuming activities.[45] It is also well known that digital divides have significant impacts on political inclusion, political knowledge, political participation and democratic institutions,[46] and digital inequality may matter even more than its analogue counterpart.[47]

Furthermore, nowadays the Internet has gradually become *a* major stage of freedom of expression in modern life, if not the one with the largest reach. At the same time, digital technologies have enabled political States to exert systematic control over online freedom of expression via various technical means, the most common being Internet access restrictions, systematic online censorship, surveillance and filtering. To achieve this, different technologies are employed such as Deep Packet Inspection (DPIs), and the blocking of services in various forms including at the network protocol level and alternatives to filtering. The tools used range from denial of service (DoS) attacks, the restriction of access to Internet domains, the selection and removal of search results, through to the taking down

41 Anita Allen, (2011) *Unpopular Privacy: What Must We Hide?*, Oxford, New York: Oxford University Press, p. 164.

42 ECJ, Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Judgment, 13 May 2014.

43 For instance, the implementation of the verdict to domain ".com" by Article 29 Data Protection Working Party. Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on «Google Spain and Inc. v. Agencia Española de Protección de Datos(AEPD)and Mario Costeja González" C-131/12, 26 November 2014, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

44 Lu Wei and Douglas Blanks Hindman, "Does the Digital Divide Matter More? Comparing the Effects of New Media and Old Media Use on the Education-Based Knowledge Gap", (2011) *Mass Communication and Society*, Vol. 14, No. 2, p. 219.

45 Alexander J.A.M. van Deursen and Jan A.G.M. van Dijk, "The Digital Divide Shifts to Differences in Usage", (2014) *New Media & Society*, Vol. 16, No. 3, p. 219.

46 Ibid., p. 230.

47 Lu Wei and Douglas Blanks Hindman, "Does the Digital Divide Matter More? Comparing the Effects of New Media and Old Media Use on the Education-Based Knowledge Gap", (2011) *Mass Communication and Society*, Vol. 14, No. 2, p. 229.

of websites.[48] Additionally, with new technical means such as those enabling 'user targeting' and 'data profiling', it is increasingly easy for States to exert control over the exercising of the right to freedom of expression; e.g. subsequent to the analysis of collected personal data, authorities may be able to locate human rights activists and limit their activities.[49]

It is not easy to describe or decide how certain kinds of online activities may or should influence the nature or exercising of the rights to freedom of expression and association online. For instance, in many democracies journalists and news reporters traditionally enjoy special legal protection relating to freedom of expression, as the fourth estate. Nowadays, given the continuous diminishing of the differences between traditional professional reporters/journalists and ordinary online informants—e.g. Internet users (or 'Netizens') who generate content by reporting live news and events, or social media producers—whether such special protection should be shared with ordinary informants on a content base is unclear and deserves further consideration of law.[50] Likewise, given that online expressions often reach far beyond national borders, it is not clear to what extent certain sorts of expressions that are totally legal and tolerable in one community—e.g. blasphemous speech, religious or anti-religious speech,[51] and posthumous defamatory speech[52]—are legally, religiously and politically acceptable in other communities and States. Also, it is sometimes debated whether Distributed Denial of Service (DDoS) attacks are a new form of freedom of expression;[53] e.g. if such DDOSs are conducted by 'hacktivists', or performed or supported by national States for political or military purposes.

In summary, the fact that the Internet has turned into a critical, principal communications medium and is a means to re-construct modern human life is clearly something that has enhanced freedom of expression. However, this has also extended or increased the old problems of abusing the right to freedom of expression, as well as created new risks and dangers to it. There is also the overarching challenge to balance online freedom of expression with other human rights and public interests in a much diversified world.[54]

2.3 Transparency and access to information: more challenges

Transparency and accountability lie at the core of good governance in relation to both modern States and private corporations. They are also central to the development of

48 William H. Dutton et al., *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*, UNESCO Series on Internet Freedom, Report, 2011, Paris: UNESCO, pp. 34-40, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-Internet/>.

49 For instance, in the recent case ECtHR, *Shimovolos v. Russia*, Judgment, 21 June 2011, Application No. 30194/09.

50 For instance, some argue to extend the definition of journalists to social media producers. See UNESCO, Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, Report, 2015, Paris: UNESCO, p. 40, available at <http://unesdoc.unesco.org/images/0023/002325/232563E.pdf>.

51 Such as anti-Islamism speech.

52 Bo Zhao, "Legal Cases on Posthumous Reputation and Posthumous Privacy: History Censorship, Law, Politics and Culture", (2014) *Syracuse Journal of International Law and Commerce*, Vol. 42, No. 1.

53 Jay Leiderman, "Justice for the PayPal WikiLeaks Protesters: Why DDoS Is Free Speech", *The Guardian*, 22 January 2013, sec. Comment is free, available at <http://www.theguardian.com/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech>.

54 The problem of balancing different rights and public interests in particular between online privacy and freedom of expression will be discussed in Chapters 6 and 7.

modern democracies.[55] Chapter 5 elaborates on the meaning of transparency—considered as a social value—and its links to the right to information. It suffices at this point to say that transparency influences the free flow of information and in brief refers, primarily, to both the availability and accessibility of information from a passive attribute and the efforts to make information easily usable from a positive perspective,[56] whether such information is held by public bodies or the private sector.

The challenges to such transparency in the digital age can be grouped in two categories. First, there is the general need for access to, and data transparency of, public information held by government authorities and private companies, if private individuals are concerned or public interests are involved. Second, there is the special need for transparency of, and access to, information regarding freedom of expression, privacy and data protection in the private sector, public sector and government bodies.

The Internet has created new options for transparency at the global level regarding the information held by government bodies, the public sector and the private sector.[57] Certainly, more transparency helps to improve the accountability of political States on the international stage with respect to the protection of human rights and public interests. Greater transparency can also contribute to peace and international security by reducing uncertainty, decrease conflicts by increasing mutual understanding between individuals and groups of individuals, decentralize global power by breaking government monopoly over information, and empower NGOs, civil society and individuals to be active in improving democracy, social justice, freedom and good governance.[58]

However, greater transparency can also generate more risks and challenges. For example, more information and transparency may lead to conflicts of values around activities regarded as immoral in some communities and encourage the victimization of out-groups. Similarly, greater transparency does not necessarily lead to good governance and democracy,[59] particularly if it does not empower those at the bottom of the power pyramid. Also, unrestricted online disclosures of critical information can cause dangers to particular communities and minorities. Thus, it is clear that the use of new ICT technologies to enable greater transparency, especially at global level, gives rise to delicate and complex issues and challenges – in particular, in striking the right balance between the interests of the whole and of particular communities, between individuals and collectives and between short- and long-term interests. In view of this, it is also clear that whilst the positive aspects of transparency must be recognised and advocated, there needs to be debate about the extent to which government-held data—in particular classified data—can be disclosed online, and with what exceptions. Such debate should take cognisance not only of national laws and mores of a particular society or power elite, but also their interpretations under international law, in particular international human rights laws and principles.

At the national level, there have been increasing calls for data transparency in relation to governmental operations, due to an increasing demand for the accountability of governments, participation in political events, anti-corruption and the establishment of

55 Definition of transparency, its historical development and values will be further discussed in Chapter 5.

56 Frederick Schauer, "Transparency in Three Dimensions", (2011) *University of Illinois Law Review*, No. 4, pp. 1343-1344, available at <http://www.illinoislawreview.org/article/transparency-in-three-dimensions/>.

57 As can be seen by how Snowden and other whistleblowers managed to connect with journalists and human rights activists to get information publicized, which is more difficult in the pre-digital age.

58 Kristin M. Lord, (2012) The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace, Albany: State University of New York Press, pp. 2-3.

59 Ibid., p. 3.

public trust; or simply because of the right to know the information held by government.[60] The global tendency towards e-governance and e-democracy has also increased transparency by contributing to the digital disclosure of government information, which, compared to its non-digital counterpart, is less costly and, in countries with ubiquitous connectivity, easier for ordinary citizens to access, thereby supporting increased participation in public affairs and the policy making process. However, the same shift towards the digitization of government information may also be combined with potential risks, such as the loss of privacy of the data subjects, threats to data protection, growing conflicts amongst participants and possibly, social fragmentation.[61] A particular problem in relation to such a shift has been the lack of transparency around national security communications surveillance. [62] The call for more transparency regarding both the work of the intelligence services and law enforcement has been for this work to meet international human rights protection standards.

The demand for transparency is increasing also in the private sector. Within this context, a significant challenge lies in the fact that, while nowadays transnational tech giants control a considerable part of the digital market under the jurisdiction of multiple State laws, it is still unclear whether such corporates can provide sufficient transparency and accountability to ensure public trust about data and privacy protection. Nonetheless, the application of transparency principles in relation to corporate conduct and governance structures, and the transparency of BCRs, as well as other measures, can improve public trust, promoting corporate reputation and improving efficiency.

A danger to transparency is the arbitrary cooperation of ICT companies with government actors, enabling such bodies to carry out massive surveillance, user data requests, restriction of access, content restriction or blocking, websites or networks blocking. In the absence of transparency, it is unknown whether such cooperation violates human rights under international standards. On many occasions, disclosure is limited due to considerations of company survival and employee safety. However, companies can use transparency to indicate their bona fides and respect for human rights in difficult contexts. The Global Network Initiative recommends that its corporate members deal with harsh political and legal environments with means such as making transparency reports and using legal appeal.[63]

Another transparency-related issue revolves around the conflicts that exist between the economic interests of ICT companies and the public interests relating to the protection of privacy and freedom of expression. Indeed, public demands for more transparency in private sector operations—to get to know the rights protection reality—may be rejected because of the economic value of information and data on the digital market.[64] For instance, data

60 Council of Europe, Electronic Democracy ("e-Democracy"), Recommendation CM/Rec(2009)1 and Explanatory Memorandum, September 2009, Strasbourg Cedex: Council of Europe Publishing, p. 77, available at <http://www.coe.int/t/dgap/democracy/Activities/GGIS/CAHDE/2009/RecCM2009_1_and_Accomp_Docs/6647-0-ID8289-Recommendation%20on%20electronic%20democracy.pdf>.

61 Ibid., p. 57.

62 Chris Tuppen, *Opening the Lines, A Call for Transparency from Governments and Telecommunications Companies*, Report, 2013, Global Network Initiative, p. 2, available at <https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf>..

63 GNI, 16-18; Chris Tuppen, *Opening the Lines, A Call for Transparency from Governments and Telecommunications Companies*, Report, 2013, Global Network Initiative, pp. 16-17, available at <https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf>.

64 See Loek Essers, "Google Ordered by German Authority to Change Privacy Practices", *PCWorld*, 8 April 2015, available at <http://www.pcworld.com/article/2907612/google-ordered-by-german-authority-to-change-privacy-practices.html>.

processing techniques, such as search engine algorithms and data analytics methods—will often be proprietary.

Similarly, under certain circumstances—for instance in the context of Cloud computing, where it is notably difficult to have a high degree of transparency[65]—the implementation of transparency principles would imply the disclosure of: data breaches; the repurposing of stored data; law compliance situations in different jurisdictions; the location, ownership and processing of the data of concern; and the related data processors' legal liabilities as such.[66] While such disclosures may often be difficult to achieve, even when there are degrees of transparency, ordinary Internet users will often not understand the information supplied to them, or be unable to identify any relevant gaps and weaknesses in the services offered to them. There is also often a lack of information of redress processes and decision-making systems.

It is nevertheless important for the private sector to strike a sustainable balance between providing the best Internet services for the users, meeting their many competing demands and securing the users' rights to privacy and freedom of expression on the one hand, while also seeking the best financial gains on the other.

In summary, the main challenge to transparency in the digital age is for the private sector, the public sector and governmental bodies to disclose more information and data about when individuals' rights to such data and information are involved. There is also a need for access to necessary information that enhances participation in democracy (or e-democracy) and e-governance. Ultimately, transparency is a collective product of all social sectors, including government bodies, the judiciary, civil society organizations, NGOs, and private companies, who can act together to enable individuals to conduct better-informed lives and to use the information available to make the best decisions.

2.4 The endangered balancing in the digital age

Before the digital world, many societies had traditional mechanisms in place that protected, regulated and balanced the interests of multiple parties relating to the collection, transfer, analysis, aggregation and processing of information. Such mechanisms have enabled stable legal and societal boundaries relating to multiple human rights, including those to privacy, reputation, freedom of expression, freedom of information, access to information and transparency. Humanity has developed the fundamental principles underpinning the rights to privacy or family life, to freedom of expression and freedom of information, which are recognized by international human rights law and regional legal instruments.[67] The balance among these values, as well as the boundaries defined between them, are set in the various legacy procedures and doctrines, legal and moral, that exist in the different legal systems and cultural communities.

The need for updating these values stems from the fact that, as shown elsewhere in this Report, ICTs challenge traditional legal and moral orders, a trend which will continue as the world moves closer to the Internet of Things, the Internet of Everything, big data analytics, Cloud computing and smart technologies.

---

65 Neil Robinson et al., "The Cloud: Understanding the Security, Privacy and Trust Challenges", Product Page, 2011, p. xi, available at <http://www.rand.org/pubs/technical_reports/TR933.html>.

66 Siani Pearson and George Yee (Eds.), (2013) *Privacy and Security for Cloud Computing*, Computer Communications and Networks, London: Springer London, pp. 15-28.

67 This will be further illustrated in detail by Chapters 3, 4 and 5.

The finding and establishment of the boundaries online is not quite the same as in the analogue world. A recent example that illustrates this is the Facebook-based conflict between a mother who has been constantly sharing information about her baby, assuming that she could express herself as much as she wanted in this new public space [68] and an individual who is assumed to be or had been connected as Facebook friend, who chose to define boundaries by sending an open anonymous letter to this mother to stop the updating,[69] indicating that s/he felt intruded with so many updates and wanted to be left alone.

There are at least two points to make regarding this situation. Firstly, in the analogue world the mother would probably have sent messages only to those whom she thinks really care about the new-born, instead of broadcasting the message to everyone connected to her as a Facebook friend. This would support the view that people react differently to online and offline environments. Secondly, the methods used to define boundaries may differ too. For instance, whilst the offended individual could—instead of sending such a letter— "de-friend" the mother, and indeed this is what often happens in such situations, such de-friending could, in one view, equate to one leaving a favourite public bar because one person at the bar has begun to dominate interactions, interrupting others who expect some silence or are accustomed to more diversified or less personal interactions.

The conflicts between privacy and freedom of expression are intensified by the combination of the virtual and physical spheres. For example, based on the information available on the online stalking and bullying cases, many individuals are the victims of the online disclosure of their personal information collected from either the online or offline environment. Nevertheless, the damage inflicted to the victim's personal life – e.g. reputational damages or lost personal relationships – has occurred both in the virtual and physical world. On some occasions, online disclosures are used specifically to punish individuals in manners that transcend both the online and the offline worlds, simply because such people hold different morals, despite individuals' behaviours that may conform to the applicable domestic laws and regulations. As an example of this, some have used online and offline disclosures of personal information to punish doctors who help pregnant women with abortion.

It may also be argued that the proliferation of portable devices that are capable of collecting, storing and transferring data such as laptops, smartphones and smartwatches, can hinder freedom of expression and opinion insofar as they threaten to facilitate the publication of private interactions. On the other hand, since such devices offer potential for increased identification and transparency they may also provide disincentives for the misuse of the right to freedom of expression; e.g. speech intended to incite hatred or violence. Therefore, technology can be seen as both potentially hindering privacy and also stifling freedom of speech and transparency.

Another challenge that emerges from the conflicts between freedom of expression and personal privacy relates to whether or not non-professional reporters and journalists—e.g. freelance reporters, citizen journalists, grassroots media and other content generators in the Web 2.0 age—should deserve the same special protections as those enjoyed by their

68 See in general Post's explanation of rules of civility in privacy protection. Robert C. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort", (1989) *California Law Review*, Vol. 77, No. 5,p. 957.

69 "Mum Sent Poison Pen Letter for Posting Too Many Baby Pics on Facebook", *Mail Online*, available at <http://www.dailymail.co.uk/news/article-3038419/She-crawls-mat-DONT-CARE-Mother-reveals-message-sent-friends-Facebook-said-sick-oversharing-information-daughter.html>, accessed 16 April 2015.

professional counterparts, for example the qualified shielding of the confidentiality of sources.[70] This issue arises in the light of the conflicts between freedom of expression and personal privacy, particularly nowadays, with respect to the reporting of issues of public interest[71], due to the free speech protection especially relied upon by journalists, and at the same time the restricted privacy protections imposed in many jurisdictions on public figures, including figures involved in the matters being reported.

A closely related challenge is that of the changing legal status of Internet intermediaries such as Internet Service Providers (ISPs), search engines and portals, social networking platforms or participative networked platforms, and data processing and web hosting providers.[72] While these intermediaries are critical to the functioning of the Internet, they are often caught in the increasingly complex dilemma of balancing (or escalating conflicts between) online freedom of expression, privacy and transparency. In addition, as many traditional media shift their services from the offline to the online environment, they become hybrid intermediaries striking ever more intricate balances, or escalating such conflicts, insofar as in shifting from the offline to the online domain they find themselves both generating content and providing a public space that enables users to generate and share content. [73]

Thus the key challenge relates to how States define these service providers and the corresponding legal duties, since such definitions will have a significant influence on the protection of privacy, freedom of expression, and freedom of information. For instance, if intermediaries are treated as media, then they usually bear stricter legal obligation to control contents. [74] In this regard, States could increasingly use intermediaries as the points of censorship.[75] Where a distinction is maintained, intermediaries are likely to be awarded limited liability for content, which means that they would be required to intervene only if notified and persuaded that the content is illegal. Courts may also hold them liable for any non-intervention relating to illegal content that persists on their platforms. Such approach would contrast the approach taken by those jurisdictions protecting even business free speech rights, like regarding search engine's algorithms as a particular category of freedom of speech protected by constitution.[76] In general, the delegation of the power for content control introduces worries linked to the privatization of law enforcement, which runs afoul

70 For instance, the constitutional and statutory protections of journalists in the U.S. law. Also see UNESCO, *Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet*, Report, 2015, Paris: UNESCO, available at <http://unesdoc.unesco.org/images/0023/002325/232563E.pdf>.

71 The balancing of the privacy interests of public figures and freedom of expression of others as a public good will be discussed further in Chapter 8.

72 In this Report, publishers and other media creating and disseminating original contents are not intermediaries. For a discussion of different categories of Internet intermediaries and their importance in network operation by the Organization for Economic Cooperation and Development (OECD), see OECD, *The Economic and Social Role of Internet Intermediaries*, Report, April 2010, pp. 6-14, available at <http://www.oecd.org/internet/ieconomy/44949023.pdf>.

73 Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom, Report, 2014, Paris: UNESCO, pp. 19-20, available at <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

74 See Ross LaJeunesse's discussion of this situation at 2014's IGF (Internet Global Forum), available at Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom, Report, 2014, Paris: UNESCO, p. 20, available at <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

75 Rebecca Ong, "Internet Intermediaries: The Liability for Defamatory Postings in China and Hong Kong", (2013) *Computer Law & Security Review*, Vol. 29, No. 3, pp. 274–281.

76 Stavroula Karapapa and Maurizio Borghi, "Search Engine Liability for Autocomplete Suggestions: Personality, Privacy and the Power of the Algorithm", (2015) *International Journal of Law and Information Technology*, Vol. 23, No. 3, p. 8.

of principles of rule of law and democracy, especially when there are commercial interests and an absence of transparency concerning content take-downs.

A popular practice among intermediaries is to provide terms of service and require the users' agreement before the use of their services, even if some contracted restrictions exceed the national legal limits.[77] In this context, how corporate practices and BCRs of privately-owned public spaces interplay with government is a decisive factor for balancing the rights to freedom of information and privacy, as well as the issue of transparency. For example, how intermediaries handle the digital legacies of dead persons—e.g. a deceased's information and data stored in the Facebook account of the deceased —now becomes a policy problem in many countries. In many cases, relatives of the deceased, even with passwords or last wills, are not allowed to access such SNS accounts when the intermediaries block access according to their terms of service.[78] This reflects that it might be the case that even the deceased have an interest in privacy, in that they might not want their private information disclosed after death, even to close family members. Thus, unlike in the pre-digital age, in several contexts it is nowadays technical giants rather than the State that have a last say over data residing on their properties. When there is no legislation to strike a good balance, "code is law" in the digital era.

Another apparently problematic issue is the conflict between the right to access to information and freedom of information, and the right to privacy. The Google Spain Case, discussed in more detail later in the study, saw the ECJ order that the link to the "irrelevant" and "outdated" information of the plaintiff, in this case an auction notice of his repossessed house, should be removed by Google Spain,[79] although the information is open to public access after being published to comply with a local law mandate and this information remains on the original website. On the one side is the privacy and reputation interest of the plaintiff and therefore an interest in delisting on Google, and on the other side is the right to freedom of expression and access to information of others. For many, it is still debatable in the long run if this decision to remove what the court deemed as irrelevant and outdated information strikes the right balance between the two fundamental interests.

Individual's rights of access to information and freedom of information must be re-considered in the digital age. The concept of freedom of information has been mostly understood as 'access to information held by governmental institutions', either by filing applications or by voluntary disclosure. But when private institutions are gradually taking more public responsibilities and thus hold increasingly more personal information that is critical to individuals, the scope of this right is overly limited if it does not cover the information or data in possession of the private sector, public sector, and government bodies. This is also the case when a huge amount of data collected by governments and State-owned enterprises is processed by private institutions that reside locally and/or abroad, such as in the context of Cloud computing.[80]

---

77 Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom, Report, 2014, Paris: UNESCO, p. 20, available at <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

78 Jessica Hopper, "Digital Afterlife: What Happens to Your Online Accounts When You Die? - Rock Center with Brian Williams", *NBC News*, 1 June 2012, available at <http://rockcenter.nbcnews.com/_news/2012/06/01/11995859-digital-afterlife-what-happens-to-your-online-accounts-when-you-die?lite>, accessed 24 May 2015.

79 Opinion of Advocate General Jääskinen in Case C-131/12 *Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD)*, delivered on 25 June 2013.

80 As in reality, some universities have outsourced their electronic communications services to companies like Google for economic reasons.

This change of the legal scenario has been considered by some national laws on freedom of information in different forms. However, the majority of State laws still need to adjust to the change of circumstances. The right to access to one's personal information has been protected under the EU law under the title of the right to data, which covers access to information regarding an individual in the private sector. More importantly, individual users have the right to know the terms of services or BCRs, particularly regarding the protection of their private data and privacy, including any information regarding the collection, storage, analysis, processing, change of purpose of use, and transfer of their data to third parties. However, in reality, many private companies are still not fully aware of their consumers' right to access to information.[81]

Individuals' lack of sufficient access to information, even their own personal information in possession of the private sector, can be further compromised by technical complexities. Even provided with required information, individuals may not be able, or do not have the time or awareness, to fully understand what happens to their data. While many ISPs require the user's consent to their terms of service, in particular those regarding privacy, data use, choice of law and choice of jurisdiction, many Internet users do not even read such texts before ticking and clicking for consent.[82]

2.5 Further indirect, but long range impacts

As outlined above, the challenges to individual privacy, freedom of expression, access to information, and transparency in the digital age are changing the traditional legal and moral boundaries developed in previous balancing mechanisms of these conflicting rights in the pre-Internet era. The intensified conflicts between the right to privacy and the right to freedom of expression reflect the fact that the pre-digital laws and morals cannot be fully and directly applied to the online world, even though it is agreed broadly, at the UN level, that human rights offline apply equally online. Indeed, it is the case that many previous legal rules and social norms need to be updated to adapt to the digital age, especially as the direct implementation of offline rules and norms to online circumstances may hinder the protection of both privacy and freedom of expression. For instance, there may be a need for tailored rules—respecting international human rights law—for governing the legal rights and duties of Internet intermediaries in view of their critical status in the operation of the Internet. Another example is the definition and legal regulation of personal data or personally identifiable data that was conceptualized in analogue times.[83] The impact of these challenges reaches far beyond national geographical borders, and will need stronger international cooperation in the long run.

In this context, certain empirical research suggests that increasing privacy invasions in the digital age are having deeper and wider impacts on individual lives and human society than most people would have expected. According to the most recent empirical research findings in Europe, the privacy invasion practices in present surveillance activities have

81 For instance, see "Belgian DPA Report Says Facebook Tracking Violates EU Law", *Daily Dashboard*, 31 March 2015, available at <https://iapp.org/news/a/belgian-dpa-report-says-facebook-tracking-violates-eu-law/>, accessed 9 September 2015.

82 Rikke F. Joergensen, "The Unbearable Lightness of User Consent | Internet Policy Review", (2014) *Internet Policy Review: Journal on Internet Regulation*, Vol. 3, No. 4, available at <http://policyreview.info/articles/analysis/unbearable-lightness-user-consent>, accessed 29 May 2015.

83 Paul M. Schwartz and Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", (2011) *New York University Law Review*, Vol. 86, available at <http://papers.ssrn.com/abstract=1909366>.

brought forth 62 specific Adverse Events (AE). These include negative impacts on: a) individual identity (12 AE); b) autonomy (12 AE), and c) reputation (7AE). They also cover impacts that impede: a) public trust (10 AE); b) quality of democracy (AE); and c) social justice (9 AE).[84] These adverse developments are not fully known by ordinary citizens, and they have not been comprehensively addressed by administrative and legal reforms.

Among the challenges to online freedom of expression is the gradually-forming position of the Internet as the public space and archive for information dissemination and data preservation. Simultaneously, it is much easier for any actor to understand both national citizens and the citizens of other countries, by collecting individual data via open source data and special surveillance channels. This can lead to freedom of expression being more easily monitored and controlled by government authorities without appropriate checks and balances.[85] The (over)exposure of an individual in the online world without adequate privacy concern can increase the possibility that the individual becomes a target and the person be subjected to data profiling.

A related concern is that private persons may have their personal data–e.g. family documents, photos, blog posts—and especially those stored somewhere in the Cloud, lost or unable to trace. While this bizarre situation is almost impossible in theory, sporadic incidents of Internet failure across the world have shown how extensive the damage could become.

Many of the challenges described certainly have an international dimension when free expression and informational privacy are conceptualized in diversified ways and protected to different extents across the world. Under international human rights law, each human being has the rights to privacy and freedom of expression, which are un-alienable and universal rights superior to national laws. However, the privacy of non-citizens is protected very differently. Additionally, in a world of data flows across borders, it does not always matter where an Internet user is. The protection of personal data and data privacy can neither be secured by domestic law, nor by international one.

Clashes over the two fundamental rights happen not only between individuals and companies, as well as individuals and national States. They may also occur between State authorities and transnational companies. Big companies may withdraw service from a State where State authority requires the provision of personal information or the blocking of certain contents and connections. At this point, certain proposed practices in the private sector, like more transparency regarding disclosure demands, responses and procedural safeguards, will help limit the threats from arbitrary State interference.[86]

84 Review of RESPECT project WP13 report by Claudia Colonnello, to be published on RESPECT's website as a deliverable of the RESPECT project. See <http://respectproject.eu/>.

85 See Evgeny Morozov, (2012) *The Net Delusion: The Dark Side of Internet Freedom*, Reprint Edition, New York: PublicAffairs, pp. 143-177.

86 Global Network Initiative, "New Report Calls for Transparency from Governments and Telecommunications Companies", pp. 16-19, available at <https://www.globalnetworkinitiative.org/news/new-report-calls-transparency-governments-and-telecommunications-companies>, accessed 13 April 2015.

2.6 The challenges of Internet Governance: increasing complexity

To protect the rights to privacy and freedom of expression, as well as to achieve transparency, including in balancing the two rights, is not an easy task in the context of the present Internet Governance structures and practices. Internet Governance issues nowadays cover a mixture of international and national problems, commercial interests and human rights protection, national State power and transnational digital giants, and an assortment of civil society organizations and whistleblowers. The multi-stakeholder governance approach is exactly a reflection of the present complex situation, in which State authority has not been the predominant player, despite the fact that its powers continue to increase in the name of protecting national security, public order and other public interests.

There are concerns about the privatization of the governance of the Internet when digital giants with considerable market shares have full discretionary power to decide who has access to what kinds of information online. Driven by commercial interests, it is hard to say how such actors, who are accountable only to shareholders, would favour the two fundamental rights of expression and privacy, especially in relation to the end users. This is reflected in the opaque privacy policies with respect to Cloud storage and content control with limited redress for citizens. On the other hand, opacity may in some cases work to protect individuals' privacy and freedom of expression.

CHAPTER 3 Online privacy and data protection mechanisms

3.1 Defining privacy in contexts

The right to privacy is a human right and the need for privacy is universal and deep-seated in each human being. For a long time, privacy has been an important subject of anthropological, sociological and philosophical discourses, about how it is defined and respected in various cultures.[87] As a concept per se, privacy has various roots, including in numerous religious texts—e.g. the Christian, Muslim and Jewish traditions—and in ancient China and Greece.[88] For the purposes of this Report, 'Privacy' may be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" without interactions from others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[89] Privacy is essential to human dignity and autonomy in all societies, enabling individuals to create barriers to protect themselves from interferences in their lives, such as access to their bodies, places and things, as well as their information and communications.[90]

Despite the ubiquity of the notion of, and the need for privacy, there is no universal definition for it.[91] The multiple ideas and conceptions conveyed can be approached from three interdependent clusters.[92] The first cluster concerns physical space, which refers to the extent to which an individual's physical space is protected from undesired invasion. The second cluster concerns making a choice, referring to an individual's ability to make certain significant decisions without external interference; i.e. to personal autonomy. The third cluster concerns 'information privacy', or the flow of personal information, and refers to an individual's control over the processing of personal information, including acquisition, disclosure, and use in different forms and for different purposes. In this third sense, the right to privacy refers to the ability of individuals to determine who has information about them and how that information is used.[93]

The concept of privacy bears various dimensions and distinct meanings in different cultural and societal contexts. As one of the fundamental and indispensable elements of human life, privacy is also closely associated with other deep-seated values, such as autonomy, dignity, spirituality, liberty, trust, reputation and personal development.[94] Furthermore, the

87 Judith DeCew, "Privacy", in *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (Ed.), Spring 2015, available at <http://plato.stanford.edu/archives/spr2015/entries/privacy/>.

88 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 50, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

89 Lord Lester of Herne Hill, Lord David Pannick and Javan Herberg (Eds.), (2009) *Human Rights Law and Practice*, Third Revised Edition, London: LexisNexis, para. 482.

90 See the general illustration by Privacy International at <https://www.privacyinternational.org/>.

91 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 9, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

92 To borrow Prof. Kang's categorization, see Jerry Kang, "Information Privacy in Cyberspace Transactions", (1998) *Stanford Law Review*, Vol. 50, pp. 1202–1205.

93 OHCHR, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, UN Doc. A/HRC/23/40, para. 22, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

94 Marc Rotenberg, "Preserving Privacy in the Information Society", *UNESCO.org*, available at <http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm>, accessed 30 May 2015..

right to privacy complements other rights and freedoms, including freedom of expression, association and belief.[95] The ability to communicate anonymously without governments knowing our identity has played a crucial role in safeguarding free expression and strengthening political accountability.[96] For this reason, the value of privacy lies in promoting and securing democracy by providing citizens with the necessary space to develop and exercise their capacities of personal reflection, judgement and action.

Privacy is unequivocally recognized as an important human right, at both the international and regional levels. However, despite the global recognition of the obligation to protect privacy, the content of this right has not been fully developed by international mechanisms for the protection of human rights.[97] The lack of explicit articulation of this right has led to difficulties in its application and enforcement.[98] Its interpretation in practice has encountered "challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest".[99]

The interplays between, and the methods used to balance privacy and other public interests, will be discussed and explained further in Chapter 6.

3.2 Information privacy and data privacy in the digital age

With advances in innovative and sophisticated technologies, public bodies and entities from the private sector can now use "automated" means to collect, process and store all kinds of personal information. For instance, when individuals use or buy all sorts of services and products—e.g. when registering for an email service, visiting a doctor, or entering into a contract—they hand in their personal information. It is in this context that data protection laws have been developed to protect personal data from being misused for illegitimate purposes.

Data protection laws are designed to protect personal information that is either intended to be part of a filing system or collected, processed and stored by "automated" means.[100] Personal information includes data attributed to an individual, such as home address, telephone number, and social security number that might be used to identify the individual,[101] as well as personal data that is generated on a sporadic basis—such as

95 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 7, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

96 Ibid.

97 OHCHR, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, UN Doc. A/HRC/23/40, para. 21, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

98 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 51, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

99 OHCHR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, *Frank La Rue*, 17 April 2013, UN Doc. A/HRC/23/40, para. 21, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

100 See Privacy International, "What Is Data Protection?", available at <https://www.privacyinternational.org/?q=node/44>, accessed 30 May 2015.

101 Thomas B. Kearns, "Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns", (1999) *William & Mary Bill of Rights Journal*, Vol. 7, No. 3, pp. 976-977, available at <http://scholarship.law.wm.edu/wmborj/vol7/iss3/10/>.

medical data, credit card purchases, phone calls—which may be used to track the subject's activities.[102] Personally Identifiable Information (PII) refers to any information, be it stored online or offline, that identifies a person, or information that is not publicly accessible and purely statistical, or information that is certain types of data defined by law as PII.[103] A much-used concept is Information privacy (or data privacy), which refers to 'a person's control over the dissemination of information about himself to others',[104] or 'the right to control one's personal data'.[105] In similar vein, information privacy '…concerns the handling of `personal information' that is, information about a particular person or information that can be used to identify a particular person….'[106]

A closely-related, important concept is 'sensitive personal data' which refers to personal data revealing racial categorization or ethnic origin, political opinions, religious or other philosophical beliefs, criminal convictions, trade union membership, and personal data concerning health or sexual life.[107]

Data protection laws empower individuals to control and protect their information from abuses and, thus, restrain and shape the activities of governments and companies.[108] Even though there is a significant overlap between data protection and privacy protection, insofar as the disclosure of data can lead to privacy breaches, data protection rules differ from privacy protection rules, both in their scope and in substantive content.[109] Some even hold that data protection law applies to all personally identifying data while privacy protection law applies to a narrower scope of information of which individuals usually have a reasonable privacy expectation, [110] though this may not be a universally-held view.

In addition, data protection rules are applied to the limited context of automated data processing or the processing of structured data sets, in contrast to privacy protection rules which can be applied to any information of a person. Moreover, data protection rules do not typically recognize a general public interest override, as witnessed in the European Union Directive 95/46/EC with specific exceptions for data processing and data transfer, and limited scope of exemptions allowed to be made by Member States.[111] Apart from these

102 Ibid.

103 Paul M. Schwartz and Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", (2011) *New York University Law Review*, Vol. 86, pp. 1828-1832, available at <http://papers.ssrn.com/abstract=1909366>.

104 Jocelyn Watkins, "My Life Is Not My Own: Do Criminal Arrestees' Privacy Interests in Mug Shots Outweigh Public's Desire for Disclosure", (2013) *John Marshall Journal of Information Technology and Privacy Law*, Vol. 30, No. 2, p. 311.

105 Lauren Henry Scholz, '"Information Privacy and Data Security", (2015) *Cardozo Law Review de Novo*, , p. 110, available at <http://papers.ssrn.com/abstract=2600495>.

106 See Australian Privacy Commissioner, "What Is Information Privacy and Why Do We Need to Protect It?," August 1997, available at <http://www2.austlii.edu.au/itlaw/national_scheme/national-PART.html>.

107 European Union Agency for Fundamental Rights (FRA), (2014) *Handbook on European Data Protection Law*, Luxembourg: Publications Offices of the European Union, pp. 43-44, available at <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law>.

108 Privacy International, "What Is Data Protection?", available at <https://www.privacyinternational.org/?q=node/44>, accessed 30 May 2015.

109 "Certain elements of data protection regimes are covered by the right to privacy". Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 101, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-internet-privacy-and-freedom-of-expression/>.

110 Ibid., pp. 101 and 105.

111 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2015, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

differences, another aspect to keep in mind is that in continental Europe it is the general practice to talk about data laws or data protection laws, while in other English-speaking countries such kinds of laws are referred to as privacy protection laws.[112] It is nevertheless the general tendency that data protection rules may have more overlaps with privacy protection rules in the context of increasing digitalization of information.

As technological advances have been influencing the nature of many societies, ICT is having an unprecedented impact on privacy, particularly on data privacy. In the digital era, these technologies have enhanced the capacity of governments, and the State now has '… greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before…'[113] Such collected information (data) can be used, abused and misused by government bodies, business institutions and individuals for any number of purposes, without the knowledge of the data subjects.[114] On numerous occasions, this can lead to privacy violations with considerable consequences on individuals' lives. In this context, it is important for individuals to exercise control over their own data, including by knowing who has access to such personal information, how personal information is processed, and for what purposes personal information is processed.[115]

Moreover, other rights, such as the right to freedom of opinion and expression, the freedom of peaceful assembly and association and to family life, may also be affected by the interception of digital communications, the collection of personal data in various forms, and different types of surveillance.[116] All these rights are connected closely with the right to privacy in the digital age and they are exercised more and more via digital media.[117]

3.3 Privacy protection mechanisms: a brief review

3.3.1 International law framework

The right to privacy, albeit not fully elaborated, is well established in international law. The core privacy principle can be found in Article 12 of the Universal Declaration of Human Rights (UDHR), and the right to privacy was given formal legal protection in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Also, the UN Human Rights Committee (HRC) states—in General Comment No. 16 on Article 17 of the ICCPR—that the

112 OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Section 'Activities at national level', available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, accessed 26 May 2015.

113 Navi Pillay, "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)", 30 June 2014, para. 2; see A/HRC/23/40, para. 33, available at <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>.

114 Thomas B. Kearns, "Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns", (1999) *William & Mary Bill of Rights Journal*, Vol. 7, No. 3, pp. 976-977, available at <http://scholarship.law.wm.edu/wmborj/vol7/iss3/10/>.

115 Navi Pillay, "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)", 30 June 2014.

116 Ibid., para. 14.

117 Ibid.

right to privacy circumscribes the right to protection '…against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons…'[118]

Regarding data protection, General Comment No. 16 states that the collection and holding of personal information must be regulated, whether such collection and holding are performed by public or private bodies. The General Comment also states that individuals have the right to acknowledge what information is kept about them, for what purposes, and by whom it is kept.[119] Furthermore, the UN General Assembly Resolution 68/167 reaffirms that: '…The exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and is one of the foundations of a democratic society…' It also expresses the UN's deep concern about the negative impacts of mass surveillance and interception of communications on human rights.[120]

In terms of the right to data protection, within the UN, the General Assembly Resolution 45/95 adopted Guidelines for the regulation of computerized personal data files,[121] which set out ten principles on data protection. While these principles are pertinent mainly to national legislation, they are also relevant to intergovernmental organizations.[122] The guidelines include a number of principles governing the collection and use of personal data, which acknowledge that there may be a need for exceptions for the first five principles, but which specify that such exceptions can only occur to protect national security, public order, health and morals, or the rights and freedom of others.[123]

In UNESCO context, it is important to note that the Organization has reaffirmed, including through the Connecting the Dots conference Outcome Document endorsed by its 38th General Conference in November 2015, that the right to privacy applies and should be respected online and offline in accordance with Article 12 of the UDHR and Article 17 of the ICCPR. As relevant within UNESCO's mandate, Organization also supports the efforts related to UN General Assembly Resolution A/RES/69/166 of December 2014 on the Right to Privacy in the Digital Age. UNESCO, as an intergovernmental organization, also works to supporting best practices and efforts made by Member States and other stakeholders to address concerns on the Internet in accordance with their international human rights obligations, and includes consider in this respect the key role played by actors in the private sector.

118 OHCHR, CCPR General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), 8 April 1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), para. 1, available at <http://www.refworld.org/docid/453883f922.html>, accessed 29 May 2015.

119 Ibid., para. 10; see also Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 52, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

120 UN General Assembly, "Resolution Adopted by the General Assembly on 18 December 2013 [on the Report of the Third Committee (A/68/456/Add.2)] 68/167. The Right to Privacy in the Digital Age", December 2013, available at <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>.

121 UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, UN Doc. A/RES/45/95, available at <http://www.un.org/documents/ga/res/45/a45r095.htm>.

122 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 63, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

123 Ibid., p. 64.

3.3.2 Regional privacy protection mechanisms

Council of Europe

The Council of Europe has defined a number of privacy protection mechanisms at the regional level. Firstly, the European Convention on Human Rights (ECHR), in Article 8, provides that everyone has the right to respect for a private and family life, a home and correspondence. Secondly, in a series of rulings the European Court of Human Rights (ECtHR) has tried to clarify the scope of the ECHR's privacy protection, government actions for potential privacy breach and further features of the right.[124] Thirdly, the Council of Europe (CoE) adopted the 'Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data'—i.e. Convention 108—which entered into force in 1985.[125]

The Convention—ratified by all EU Member States and amended to enable the EU to become a Party, and having all Member States of the CoE Contracting Parties by 2014, as well as Uruguay as the first non-European country to become such a party (acceded in 2013)[126]—is the only international treaty across the world for privacy protection. Its purpose is "…[t]o secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')". In line with this, the Convention fulfils a number of functions, including those of: a) regulating abuses relating to the collection, processing and cross-border transfer of data; b) prescribing principles of data collection and processing, such as regarding: i) the fair and lawful collection and automatic processing of data; ii) the storage of data for specified legitimate purposes; and iii) the quality of data; c) granting each data subject the right to know the storage of his/her personal information, as well as the right to correct personal information when necessary; and d) providing several exceptions, justified by overriding interests such as those of State security and defence.

European Union

The protection of fundamental human rights is one of the basic tenets of EU law.[127] The adoption of the Lisbon Treaty in late 2009 provided a strong legal ground for the development of a "clear and effective" data protection system.[128] Through a number of amendments of the Treaty, the *Charter of Fundamental Rights of the European Union* became legally binding,[129] the Union acceded to the European Convention of Human Rights,[130] and

124 Ibid., pp. 54-55.

125 Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, ETS No. 181, available at <http://conventions.coe.int/Treaty/EN/Treaties/HTML/181.htm>, accessed 30 May 2015.

126 FRA, (2014) *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union, pp. 16-17, available at <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf>.

127 European Parliament, "Respect for Fundamental Rights in the Union", available at <http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_2.1.2.html>, accessed 30 May 2015; see Article 2 of the Treaty of the European Union: "the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect of human rights, including the rights of persons belonging to minorities."

128 Ibid.

129 Article 6 Paragraph 1, Treaty of the European Union.

130 Article 6 Paragraph 2, Treaty of the European Union.

the fundamental rights guaranteed by the ECHR became binding principles of the Union law.[131] Another important change is that the protection of personal data has been recognized as a fundamental right under Article 16 Paragraph 1 of the *Treaty on the Functioning of the European Union* (TFEU).

The core EU secondary legislation on the protection of personal data is Directive 95/46/EC, which lays down that Member States shall protect fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect of the processing of personal data.[132] The Directive applies to data processed by automated means and data contained in or intended to be part of non-automated filing systems. However, it does not apply to the processing of data in the course of '…operations concerning public security, defence, State security […] and the activities of the State in areas of criminal law…'[133]

Another important legal instrument at the European Union level is the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[134] Although this area is not covered by Directive 95/46/EC, the Framework Decision generally echoes the provisions of the Directive.[135] It aims at providing protection for the personal data of natural persons when such data are processed for preventing, investigating, detecting or prosecuting a criminal offence, or exacting a criminal penalty[136]. These EU legal instruments are now set to be replaced and enhanced by the General Data Protection Regulation and a Directive on data protection in the criminal justice sector approved by the European Parliament on 14th April 2016.

Other regional privacy protection frameworks

The African Charter on Human and Peoples' Rights (ACHR) does not contain elaborated protection for privacy. The relevant provisions of the ACHR state the following: "…No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks".[137] The Economic Community for West African States (ECOWAS) has a legal framework on personal

131 Article 6 Paragraph 3, Treaty of the European Union.

132 See Article 1Paragraph 1, Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

133 The Directive shall not apply either "in the course of an activity which falls outside the scope of Community, such as (…) operations concerning public security, defence, state security…." (Article 3 Paragraph 2, Directive 95/46/EC).

134 "Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters", January 2009, available at <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008F0977>. The legal bases for this measure are Articles 30, 31 and 34, Treaty of the European Union.

135 Paul De Hert and Vagelis Papakonstantinou, "The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters - A Modest Achievement However Not the Improvement Some Have Hoped for", (2009) *Computer Law & Security Review*, Vol. 25, No. 5, p. 237.

136 FRA, (2014) *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union, p. 149, available at <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf>.

137 African Charter on Human and Peoples' Rights, available at <http://www.achpr.org/instruments/achpr/>.

data protection, namely, the Supplementary Act A/SA. 1/01/10, which aligns with much of the EU Data Protection Directive (95/46/EC).[138]

Article 11 of the American Convention on Human Rights prescribes that: "Everyone has the right to have his honor respected and his dignity recognized. No one may be the object of arbitrary or abusive interference with his private life, his family, his home or his correspondence, or of unlawful attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks".

The General Assembly of the Organization of American States (OAS) adopted Resolution 2661 (XLI-O/11) on Access to Public Information and Protection of Personal Data.[139]

The main Asia-Pacific Economic Cooperation (APEC) rules on privacy can be found in the APEC Privacy Framework, which addresses the need to preserve consumer trust in order to advance economic benefits from electronic commerce. It also acknowledges the need to grant countries flexibility regarding the implementation. The key principles in the framework resemble the UN Guidelines, OECD and European standards. However, as opposed to the European standards, the Framework contains a particular degree of flexibility.[140]

3.3.3 National legal frameworks

Privacy law

The right to privacy as a human right has been recognized by most countries across the world and is protected by various legal mechanisms and legal instruments. The right to privacy is first recognized as a constitutional right against the interference from State authorities with private life. For instance, though the right to privacy was not originally written into the USA's Constitution, it was later developed from different constitutional amendments, including the First, the Second, the Third, the Fourth, the Fifth, the Eight, the Ninth, and the Fourteenth.[141]

Most European countries—following the EU basic law, the Charter of Fundamental Rights and the European Convention of Human Rights (ECHR)—recognize the fundamental right to privacy in their constitutions, in different forms. For instance, the right to privacy and private family life is protected by German constitution under the rubric of "personality right" in particular, and the right to dignity in general under Articles 1 and 2 of the Basic Law. The constitutional personality right protects the personal sphere or "essential sphere of privacy" within which an individual can decide who s/he is and how s/he is related to the

138 Graham Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108", (2011) *International Data Privacy Law*, Vol. 2, No. 2, available at <http://papers.ssrn.com/abstract=1960299>.

139 "AG/RES. 2661 (xli-O/11) Access to Public Information and Protection of Personal Data" (General Assembly of the UN, 7 June 2011), 2, available at <http://www.networkworld.com/news/2012/012612-privacy-scandals-255357.html>.

140 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 65, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

141 The Ninth Amendment prescribes that «…enumeration in the Constitution of certain rights shall not be construed to deny or disparage other rights retained by the people.» See Anita Allen, (2011) *Privacy Law and Society*, Second Edition, Minneapolis: West Academic Publishing.

rest of the world, and "personality right includes protection of information privacy". [142] The German Federal Constitutional Court has derived a constitutional right to "informational self-determination" from Article 2 Paragraph 1 containing the general personality right of the Basic Law in 1983.[143]

Privacy invasions can be tackled using a variety of legal instruments, including contractual obligation, criminal offenses, tort liabilities, defamation tort, and confidentiality responsibilities. Contractual obligation is one of the most important legal instruments for protecting individual privacy in that, for instance, Internet Service Providers must fulfil certain contractual duties previously agreed by both parties of a contract. The violation of such duties would infer legal consequences, mostly in the form of economic loss. Such obligations are mostly provided by privacy clauses in terms of service in consumer contracts. For instance, banks have the contractual duty to prevent consumer's personal data from being disclosed without the consumers' consent. Upon data breaches that lead to privacy invasion, victims can resort to contractual liability for remedies and/or damages.

Data Protection law

Nowadays, over 100 countries around the world have enacted comprehensive data protection legislation, and many other countries are in the process of passing such laws. Moreover, countries not having comprehensive data protection legislation may have privacy laws applicable to certain sectoral areas, including those of child protection or financial records.[144] Data protection law is the most used legal instrument to protect personal data and provides more comprehensive privacy protection. EU Member States have transposed the EU Data Protection Directive 95/46/EC into domestic laws, which include detailed rules covering the whole scope of data processing, including lawful data processing, code of conducts, notification duty of data processors, data subjects' rights, data transfer to third non-EU countries and the setting up of data protection supervising bodies.[145] Outside Europe, many jurisdictions have passed data protection laws or similar laws that secure data privacy.[146]

Other legal instruments

Criminal law is a strong legal instrument to tackle privacy invasion. Online privacy invasion can be punished by criminal law when other people's information is hacked and considerable harm is caused. For instance, in Virginia, USA, a person is guilty of the crime of Computer Invasion of Privacy when he or she "uses a computer or computer network

142 Edward J. Eberle, "Human Dignity, Privacy, and Personality in German and American Constitutional Law", (1997) *Utah Law Review* , p. 976.

143 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 2, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

144 Privacy International, "What Is Data Protection?", available at <https://www.privacyinternational.org/?q=node/44>, accessed 30 May 2015.

145 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, accessed 26 April 2015.

146 Graham Greenleaf, "Global Data Privacy Laws: 89 Countries, and Accelerating", (2012) *Privacy Laws & Business International Report*, No. 115, available at <http://papers.ssrn.com/abstract=2000034>.

and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person".[147]

Privacy tort is an important legal instrument to protect privacy in many legal systems, but not limited to common law jurisdictions. In the USA privacy tort traditionally covers four categories of actionable offenses, namely: a) appropriation of name and likeness; b) false light; c) disclosure of personal information; and d) intrusion of solitude and seclusion.[148] Of these, the first three can be generally applied for the protection of privacy in online contexts. Similarly, the tort of defamation can be used to protect online privacy, indirectly, because of the frequent links between an individual's reputation and privacy. For instance, private information might contain secrecies of an individual whose disclosure may have great influence on one's reputation, as well as cause economic loss and psychological distress.[149] In some circumstances, privacy and libel, the two legal avenues of complaint, seem to be merging into one big "protection of reputation lump".[150] Also there are the overlaps between false light and defamation as observed in legal practices.[151]

Since 2008 there has been a marked increase in criminal defamation cases in the new media environment.[152] However, many jurisdictions do not apply criminal defamation law in practice, leaving the crime merely on paper.[153]

Other legal instruments include a law of confidentialities in different professions including, amongst others, medical service, legal services, consulting services, banking services, and journalism. For such professions and vocations, privacy protection is central to mutual trust between the parties involved and the functionality of these private and public services. For example, lawyers are required by law not to disclose their clients' personal information to third parties if disclosure may counter the interests of their clients. Journalists in many jurisdictions enjoy some privilege not to disclose the sources of information, in order to protect informants and promote future disclosures that promote transparency and democracy. Recognition of this underpins UNESCO's position that in the digital age there is a need for enhanced protection of the confidentiality of journalism sources.[154]

In addition, there are sectoral laws and regulations to protect the privacy and private life of individuals coming from special social groups—especially when such individuals would be in a much weaker position, for various reasons—from invasion by others. For instance, the Children's Online Privacy Protection Act of 1998 (COPPA) is a USA Federal law that imposes certain requirements on operators of websites or online services directed at children under 13 years of age, and on operators of other websites or online services that have actual

147 Under 18.2-152.5 of VIRGINIA COMPUTER CRIME ACT, at *Virginia Computer Crimes Act (Excerpts)*, available at <http://courses.cs.vt.edu/professionalism/Crime/virginia.law.html>, accessed 26 April 2015.

148 William L. Prosser, "Privacy", (1960) *California Law Review*, Vol. 48, No. 3, p. 383.

149 Richard A. Posner, "Privacy, Secrecy, and Reputation", (1978) *Buffalo Law Review* Vol. 28, p. 1.

150 Siobhain Butterworth, "Privacy, Libel or Protection of Reputation?", *The Guardian,* 8 April 2011, available at <http://www.guardian.co.uk/law/butterworth-and-bowcott-on-law/2011/apr/08/privacy-libel-protection-of-reputation>.

151 Nathan E. Ray, "Let There Be False Light: Resisting the Growing Trend Against an Important Tort", (1999) *Minnesota Law Review,* Vol. 84, p. 715.

152 Mei Ning Yan, "Criminal Defamation in the New Media Environment - the Case of the People's Republic of China", (2011) *International Journal of Communications Law and Policy*, No. 14.

153 International Press Institute, *Out of Balance: Defamation Law in the EU and Its Effect on Press Freedom*, Report, July 2014, available at <http://www.freemedia.at/ecpm/defamation-law-report.html>.

154 Outcome Statement of CONNECTing the Dots, endorsed in Resolution 53 at UNESCO's 38th General Conference: http://unesdoc.unesco.org/images/0023/002340/234090e.pdf

knowledge that they are collecting personal information online from a child under 13 years of age.[155]

Other privacy protection legal instruments include special privacy clauses in multiple laws and regulations in other regulatory contexts. For instance, there may be special clauses governing law enforcement actions in searching suspects during crime investigation, and particular privacy rules in healthcare systems for privacy protection, such as the privacy rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA, which regulates the use and disclosure of Protected Health Information (PHI) possessed by covered entities.

3.3.4 Alternative instruments

In addition to the examples of legal protection instruments listed above, one can find in the private sector alternative means, which also play an important role in protecting the privacy of data subjects. As elaborated below, these include various instruments, such as self-regulation, co-regulation, market mechanisms for privacy protection, user empowerment measures, nudging mechanisms and professional ethics.

The first two (i.e. self-regulation and co-regulation) are often regarded as important means for the protection of privacy in the private sector. Self-regulation refers to situations when a non-State group engages in a rule-making process, by developing a set of rules, such as codes of conduct, a process of enforcement of the rules, or a comprehensive regulatory system altogether. It is supposed to replace the procedural, substantive, and implementation functions that might otherwise be included in State legislation/regulation.[156] Self-regulation institutions use such tools as codes of conduct and privacy seals to protect the users' privacy and improve mutual trust in privacy protection.[157, 158] For instance, the US Federal Trade Commission's moving for direct regulation, in 1998, by issuing a set of *Guidelines for Online Privacy Policies*, has led to the formation of the Online Privacy Alliance (OPA) in the mid-1990s, a group consisting of Internet firms.[159]

Co-regulation implies that State regulation and self-regulation cooperate together in the regulation of particular activities, with the State on the one hand providing a legal framework that enables the creation, operationalization and enforcement of rules, and self-governing bodies on the other hand creating rules and administering them, sometimes through joint structures or mechanisms.[160]

Regarding the third instrument (i.e. market mechanisms for privacy protection), market solutions can improve privacy protection by means of market competition. Private companies can improve their market position by competing with rivals in providing greater

155 Federal Trade Commission, "Children's Online Privacy Protection Rule ('COPPA')", available at <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>, accessed 26 April 2015

156 Ibid., pp. 197-200.

157 Jedidiah Bracy, "Will Industry Self-Regulation Be Privacy's Way Forward?", *The Privacy Advisor*, available at <https://privacyassociation.org/news/a/will-industry-self-regulation-be-privacys-way-forward/>, accessed 27 April 2015

158 Norman E. Bowie and Karim Jamal, "Privacy Rights on the Internet: Self-Regulation or Government Regulation?", (2006) *Business Ethics Quarterly*, Vol. 16, No. 3,pp. 323-342.

159 Dennis D. Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation?", 2010, p. 34, available at <http://works.bepress.com/dennis_hirsch/1>.

160 Jeanne P. Mifsud Bonnici, (2008) *Self-Regulation in Cyberspace*, The Hague: T.M.C. Asser Press, pp. 15-16.

privacy protection. When users are not demanding more privacy protection, following the theory, users value the service provided on market more than the privacy they are losing, so that there is no urgent need for regulatory interference.[161]

The fourth instrument—user empowerment measures—refers to users who may favor the use of empowering measures to protect their personal information and privacy on the Internet, including by encrypting sensitive personal data (particularly in the context of Cloud computing such as by participating in such initiatives as the Cloudprotect project[162]) —or by using Tor and GNUnet technologies.

The fifth instrument—nudging mechanisms—refers to a recent tendency for governments to facilitate tools of a soft-paternalism nature—i.e. commercial nudging mechanisms—designed to improve consumers' privacy self-protection online by "ameliorating" their privacy decisions.[163] An example of this is an alert to inform smartphone users of the privacy risk of storing sensitive personal data in certain locations or using certain apps that appropriate unnecessary private data.[164]

The sixth - professional ethics - refers to the use of constructs, such as codes of ethics, which act as moral bindings on data controllers and data processers to take the data subject's privacy into account. As an example of this, already mentioned earlier, some professions—e.g. lawyers, doctors, accountants, spiritual leaders and journalists—are bound to protect the data subject's privacy, by not disclosing confidential information, unless justified to do so in accordance with international legal standards, in order to ensure the trust necessary to support their general functioning.

3.3.5 Legitimate exceptions

The right to privacy is not an absolute right and must be balanced with other human rights and values; there are lawful exceptions to restrict the right to privacy whether online or offline. To what extent such legitimate purposes or ends may compromise the right to privacy will be case-dependent in diverse socio-legal contexts. However, there are certain general exceptions recognized by most legal systems, although their expressions or terms may differ. Unlike the right to freedom of expression as described in the ICCPR, Article 17 of the ICCPR does not provide an explicit limitation clause for privacy. Consequently, the related limitations have to be found from multiple sources; mainly the Universal Declaration of Human Rights, the Siracusa Principles, general comments by the Human Rights Committee, regional and national case law and the views of independent experts.[165] Following these authoritative sources, any legitimate limitations of the right to privacy by State authority,

161 Ibid, p. 25.

162 M.H. Diallo et al., "CloudProtect: Managing Data Privacy in Cloud Applications", in (2012) *2012 IEEE 5th International Conference on Cloud Computing (CLOUD)*, pp. 303-310.

163 Wainer Lusoli et al., *Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management*, JRC Scientific and Policy Report, European Commission, Joint Research Center, 2012, Luxembourg: Publications Office of the European Union, pp. 17-18, available at <http://is.jrc.ec.europa.eu/pages/TFS/documents/EIDSURVEY_Web_001.pdf>.

164 Rebecca Balebako et al., "Nudging Users towards Privacy on Mobile Devices", in *Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*, 2011, p. 2, available at <http://www.researchgate.net/profile/Pedro_Leon6/publication/268199850_Nudging_Users_Towards_Privacy_on_Mobile_Devices/links/548f29130cf2d1800d862282.pdf>.

165 Navi Pillay, "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)", 30 June 2014, para. 22.

when balancing with other rights and freedoms, must be in accordance with the principles of legality, necessity and proportionality to achieve legitimate aims.[166]

In legal practice, there are thematic limitations on the right to privacy that are generally accepted and integrated in national laws in most democracies around the world. For instance, under the EU Data Protection Directive (DPD), exemptions or derogations are allowed when the use of data is solely for journalistic purposes or for artistic or literary expression. This is on the condition that the actors concerned will reconcile the right to privacy with the rules governing freedom of expression, and that the actors apply such exemptions and derogations according to law and respect the principle of proportionality in a democracy. Other exceptions are also allowed under European State laws regarding matters of: (a) national security and defence; (b) public security; (c) the prevention, investigation, detection and prosecution of criminal offences; (d) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (f) the protection of data subjects and the rights and freedom of others.[167] The above exemptions cover most legitimate grounds that are allowed to compromise the right to privacy of data subjects and may be recognized to different extents in other jurisdictions.

There are sometimes certain special contexts and reasons to limit the right to privacy of specific individuals. For instance, public figures or public celebrities, in particular political figures, may enjoy more restricted privacy protection by law and/or custom than other ordinary citizens because of the public status they occupy and the corresponding influence they have on others, especially when the issues at stake are of public interest, or of a legitimate concern to the public. Even in a jurisdiction that grants comparatively strong privacy protection to public figures, there are still many limitations on the activities of such figures if such activities are of public interest.[168] The USA Restatement of Torts (Second) did recognize that public figures have some expectation of privacy, but it clarified that the scope of tort liability depends on the plaintiffs' status, further observing that: "the common law of privacy has always embraced the public/private figure distinction and that the Court has used the doctrine in a related area—the individual's right of informational privacy against the government".[169]

As suggested in the case of public figures, the protection of individual privacy is not absolute and must be balanced with other equally important values and public interests. How to optimize these values in particular circumstances, especially in case of public figures, will be discussed further in Chapter 7, in which we explore the interplays (and balancing) of privacy, transparency and freedom of expression.

166 For detailed explanations of the three principles, see Ibid., para. 23.

167 Recital 37, Article 9 and Article 13 Restrictions and exemptions. See Directive 95/46/EC. (Though the right to data protection is different from the right to privacy, the overlap of the protection is obvious in this context.)

168 Scott. J. Shackelford, "Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures", (2012) *American Business Law Journal*, Vol. 49, No. 1,pp. 72-75.

169 Susan M. Gilles, "Public Plaintiffs and Private Facts: Should the Public Figure Doctrine Be Transplanted into Privacy Law", (2005) *Nebraska Law Review* Vol. 83, No. 4, pp. 1205 and 1214.

3.3.6 Cross-border data transfer

National States may be sufficiently capable to protect the information privacy or data privacy of their own citizens within their own territories. However, as cross-border data transfers continue to prevail and to be unavoidable for the well-functioning of the Internet, it is increasingly challenging for States to protect their citizens' data privacy, especially in the case of large trans-border data flows. This challenge relates to conflicts of national laws and jurisdictions that present issues of a political and diplomatic, rather than legal, nature. As with poor international protection of data privacy, the same phenomenon on an extraterritorial basis, may lower general trust in the Internet, and it may also further lead to fragmentation of the Internet. International society has made considerable efforts to cope with the challenge, as elaborated below.

In 2000, the European Commission adopted the *Decision 520/2000/EC*—i.e. the 'Safe Harbour decision'—recognizing the Safe Harbour Privacy Principles and Frequently Asked Questions and providing adequate protection for the purposes of personal data transfers from the EU. The Decision allowed the free transfer of personal information from EU Member States to companies in the USA,[170] which had signed up to the Principles in circumstances where such data transfers would otherwise—given the substantial differences in privacy regimes between the two sides of Atlantic—not meet the EU standards for adequate levels of data protection.[171] After the Snowden revelations, the ECJ invalidated the Safe Harbour Program,[172] and a new round of negotiations had led to a "Privacy Shield" arrangement at the time of writing this report.[173]

Members of the Asia Pacific Economic Cooperate (APEC) have made developments in completing the Cross-Border Privacy Rules (CBPR) system for the protection of personal data throughout the Asia-Pacific area.[174] The system, which is based on a similar approach to EU BCR, employs internal binding rules for cross-border transfers of personal data that are subject to prior approval by EU Data Protection Authorities or by APEC-recognized Accountability Agents. These requirements are designed to align a company's privacy policies with certain established standards for the protection of personal information,[175] which must be validated by APEC-recognized Accountability Agents.[176]

The Organization for Economic Co-operation and Development (OECD) has also brought its contribution to protecting privacy through its recently-revised non-binding *Guidelines*

170 The above does not exclude the application to the data processing of other requirement that may exist under national legislation implementing the EU data protection directive; also data transfers from the three States Parties to the EEA are similarly affected, following extension of Directive 95746/EC to the EEA Agreement, Decision 38/1999 of 25 June 1999, OJ L 296/41, 23/11/2000.

171 See <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf>.

172 ECJ, C-362/14 Maximillian Schrems v. Data Protection Commissioner, Judgment, 6 October 2015.

173 Michelle Gyves, "How Safe? The Future of the US-EU Safe Harbor", *Privacy Law Blog*, 31 March 2015, available at <http://privacylaw.proskauer.com/2015/03/articles/european-union/how-safe-the-future-of-the-us-eu-safe-harbor/>.

174 Asian-Pacific Economic Cooperation (APEC), "APEC Cross-Border Privacy Rules System", available at <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx>, accessed 26 May 2015.

175 "Promoting Cooperation on Data Transfer Systems between Europe and the Asia-Pacific - Asia-Pacific Economic Cooperation", available at <http://www.apec.org/Press/News-Releases/2013/0306_data.aspx>, accessed 26 May 2015.

176 Ibid.

on the Protection of Privacy and Trans-border Flows of Personal Data.[177] Another area of the OECD's work in relation to information privacy lies in its efforts to improve cross-border co-operations amongst privacy law enforcement authorities by proposing, in 2007, an OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.[178]

177 The new Guidelines constitute the first update of the original 1980 version that served as the first internationally agreed upon set of privacy principles, see OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – OECD, available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, accessed 26 May 2015.

178 OECD, "OECD Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy", available at <http://www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm>, accessed 26 May 2015.

CHAPTER 4 Online freedom of expression and protection mechanisms

4.1 Defining freedom of expression

The term 'freedom of expression' has existed since ancient times and has been widely used and conceptualized by various groups, including scholars, politicians, activists, and laypersons.[179] With the advance of civilization and politics, in particular since the 20th century, there have been commonly agreed understandings of freedom of expression.[180] Its value and importance to individuals and society have been recognized among different communities and it has gained legal protection both under international human rights law and national State laws across the world.[181]

Freedom of opinion and expression is an essential pre-requisite in a free and democratic society.[182] It supports a free flow of ideas that guarantees public accountability and transparency, and ensures the free exercise of civil and political rights by a well-informed and empowered public.[183] In addition, freedom of opinion and expression enables societies to achieve stability and adaptability,[184] and is crucial for the development of individuals,[185] assuring their self-fulfilment,[186] including by allowing them to pursue and search for truth and knowledge.[187]

Freedom of opinion and expression is protected under Article 19 of the ICCPR. It includes the protection of the right to hold opinions without interference, as well as the right to change an opinion whenever and for any reasons a person so freely chooses. [188] Moreover, such freedom includes the right to seek, receive and impart information and ideas regardless of frontiers.[189] This implies rights both to send and to receive information. In this second respect, freedom of opinion and expression is taken as embracing the right of access to information held by public bodies regardless of the form in which the information is stored, its source or the date of production.[190]

---

179 UNESCO, (2013) *Freedom of Expression Toolkit: A Guide for Students*, Paris: UNESCO, p. 12, available at <http://unesdoc.unesco.org/images/0021/002186/218618E.pdf>.

180 Ibid.

181 Ibid.

182 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 1, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

183 Navi Pillay, "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)", 30 June 2014, para. 2.

184 UNESCO, (2013) *Freedom of Expression Toolkit: A Guide for Students*, Paris: UNESCO, p. 13, available at <http://unesdoc.unesco.org/images/0021/002186/218618E.pdf>.

185 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 1, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

186 UNESCO, (2013) *Freedom of Expression Toolkit: A Guide for Students*, Paris: UNESCO, p. 13, available at <http://unesdoc.unesco.org/images/0021/002186/218618E.pdf>.

187 Ibid.

188 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 9, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

189 Ibid., para. 11.

190 Ibid., para. 18. Freedom of access to information has a different historical or political root different from the political interpretation. See a detailed discussion of the concept of freedom of information (FOI) in Chapter 5.

The scope of information protected under this right covers information from political discourse,[191] commentary on one's own[192] and on public affairs,[193] canvassing,[194] discussion of human rights,[195] journalism,[196] cultural and artistic expression,[197] teaching,[198] and religious discourse;[199] and it may also include commercial advertising.[200] Additionally, the scope of Paragraph 2 of the ICCPR includes expressions that may be regarded as deeply offensive by some actors.[201] Moreover, the ICCPR protects all forms of expression, including spoken, written, sign language and non-verbal expressions such as images and objects of art,[202] and all means used for the dissemination of such expressions, including books, newspapers,[203] pamphlets,[204] posters, banners,[205] dress and legal submissions;[206] as well as all forms of audio visual, electronic and Internet-based modes of expression.[207] However, as elaborated below, the provisions of Articles 19, Paragraph 3, and Article 20 of the ICCPR may limit other expression under certain exceptional conditions.[208]

In particular, the universal right to freedom of opinion and expression embraces the protection of freedom of the press. A free, uncensored and unhindered media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other rights.[209] The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential, and this implies

191 HRC, *Essono Mika Miha v. Equatorial Guinea*, Communication No. 414/1990, UN Doc. CCPR/C/51/D/414/1990 (1994).

192 HRC, *Anthony Fernando v. Sri Lanka*, Communication No. 1189/2003, UN Doc. CCPR/C/83/D/1189/2003 (2005).

193 HRC, *Patrick Coleman v. Australia*, Communication No. 1157/2003, UN Doc. CCPR/C/87/D/1157/2003 (2006).

194 "Concluding Observations on Japan (CCPR/C/JPM/CO/5)", available at <http://www.nichibenren.or.jp/library/ja/kokusai/humanrights_library/treaty/data/CO_JPRep6_ICCPR140820.pdf>, accessed 23 August 2015.

195 HRC, *Mr. Vladimir Velichkin v. Belarus*, Communication No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

196 HRC, *Mavlonov and Sa'di v. Uzbekistan*, Communication No. 1334/2004, UN Doc. CCPR/C/95/D/1334/2004 (2009).

197 HRC, *Hak-Chul Shin v. Republic of Korea*, Communication No. 926/2000, UN Doc. CCPR/C/80/D/926/2000 (2004) (2004).

198 HRC, *Ross v. Canada*, Communication No 736/1997, UN Doc. CCPR/C/70/D/736/1997 (2000).

199 Ibid.

200 "[…] Information of a commercial nature cannot be excluded from the scope of Article 10, para. 1, which does not apply solely to certain types of information or ideas or forms of expression". See ECtHR, *Mark Intern Verlag GMBH and Klaus Beermann v. Germany*, Judgment, 20 November 1989, Application No. 10572/83, para. 26; see also Council of Europe Publishing, "Freedom of Expression in Europe, Case-Law Concerning Article 10 of the European Convention on Human Rights", Human Rights Files, No. 18, March 2007, para. 79, available at <http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-18%282007%29.pdf>.

201 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 11, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>..

202 HRC, *Hak-Chul Shin v. Republic of Korea*, Communication No. 926/2000, UN Doc. CCPR/C/80/D/926/2000 (2004) (2004).

203 HRC, *Ernst Zundel v. Canada*, Communication No. 1341/2005, UN Doc CCPR/C/89/D/1341/2005 (2005) (2005).

204 HRC, *Mr. Vladimir Velichkin v. Belarus*, Communication No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

205 HRC, *Kivenmaa v. Finland*, Communication No. 412/1990, UN Doc. CCPR/C/50/D/412/1990 (1994).

206 HRC, *Anthony Fernando v. Sri Lanka*, Communication No. 1189/2003, UN Doc. CCPR/C/83/D/1189/2003 (2005).

207 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 12, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

208 Ibid.

209 Ibid., para. 13.

that a free press is able to comment on public issues without censorship to inform public opinion.[210] In addition, Articles 19 and 25 of the ICCPR provide a right whereby the media has access to information on public affairs,[211] and the right of the general public to receive media output.[212] It is in the light of these dimensions that UNESCO conceptualizes press freedom as a corollary of the right to expression.[213]

Furthermore, the protection of journalists and press freedom is an issue of central importance for the full exercise of freedom of opinion and expression, insofar as journalism is a necessary activity in any society, providing individuals and society as a whole with essential information to allow them to develop their own thoughts as well as their conclusions and opinions.[214] Journalists—including media workers, support staff, as well as community media workers and the so-called 'citizen journalists' especially in the digital age—observe, describe and analyse events, statements, policies, and any propositions that can affect and shape society.[215] Moreover, journalists play a significant watchdog role in society by scrutinizing the government and other entities, as well as by providing necessary information to individuals. This enables individuals, by exercising the right to "seek and receive information", to make informed decisions and express their opinions freely and participate actively in a democratic society. [216]

Nowadays, journalists across the world continue to face risks and challenges in undertaking their professional work, despite the existence of provisions in international human rights law, which protect the journalists' right to seek, receive and impart information and ideas of all kinds.[217] These risks and challenges range from restrictions of movement, deportations and denial of access to a country; to arbitrary arrests and detention; torture and other cruel, inhuman or degrading treatment or punishment; confiscation of and damages to equipment; illegal surveillance and office break-ins; information theft; death threats; stigmatization or campaigns to discredit journalists; and abductions or enforced disappearance to killings.[218] One of the biggest challenges to ensuring the protection of journalists is impunity, or the failure to bring to justice the perpetrators of such human rights violations.[219] These issues are of great concern to UNESCO, which leads the UN Plan of Action on the Safety of Journalists and the Issue of Impunity, and has a range of activities and mechanisms on these issues.

---

210 See "Human Rights Committee General Comment No. 25 (1996) on Article 25 (Participation in Public Affairs and the Right to Vote) Supplement No. 40, Vol. I (A/51/40) (Vol. I)", n.d., para. 25, available at <http://www.refworld.org/pdfid/3f474adb4.pdf>.

211 HRC, *Robert W. Gauthier v. Canada*, Communication No. 633/1995 CCPR/C/65/D/633/1995 (1995).

212 HRC, *Mavlonov and Sa'di v. Uzbekistan*, Comm. 1334/2004, UN Doc. CCPR/C/95/D/1334/2004 (2009).

213 UNESCO, World Trends in Freedom of Expression and Media Development. 2014 http://unesdoc.unesco.org/images/0022/002270/227025e.pdf

214 Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 16 May 2011, UN Doc. A/HRC/17/27, para. 3, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27>.

215 UNESCO, "Safe to Speak: Securing Freedom of Expression in All Media", 29 May 2015, p. 7, available at <http://webcache.googleusercontent.com/search?q=cache:DDV1GWAmbukJ:www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/all-news/news/news_item_for_world_press_freedom_day/+&cd=1&hl=en&ct=clnk#.VWhUL-fD7dI>.

216 OHCHR, *Report of the Special Rapporteur to the Human Rights Council on the Protection of Journalists and Media Freedom*, 4 June 2012, UN Doc. A/HRC/20/17, para. 3, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G12/137/87/PDF/G1213787.pdf?OpenElement>.

217 Ibid. para. 48.

218 Ibid.

219 Ibid., para. 65.

In general, freedom of opinion and expression is a pre-requisite for the full exercise of other human rights.[220] For example, it is a guarantor of free and fair electoral processes.[221] It also enables a well-informed and empowered public to freely exercise its civil and political rights, and creates the conditions for a free and open political communication, which is an essential element to ensure fair and democratic electoral processes. [222] Moreover, it interrelates with the right to privacy. For instance, respect for privacy of communications is a prerequisite for trust by those engaging in communicative activities, which is successively a pre-condition for the exercise of the right to freedom of expression.[223] The interplay of freedom of expression and opinion and privacy will be discussed further in Chapter 6.

Previously, the right to freedom of expression has not been connected with the protection of children's rights. International legal instruments dealing with children's rights—such as the Geneva Declaration on the Rights of the Child of 1924 and the Declaration of the Rights of the Child[224]—have not included any reference to the issue, assuming that given their immaturity children were not able to make meaningful choices.[225] In contrast, the Convention on the Rights of the Child (CRC) proclaims the right to children to freedom of expression.[226] Article 13 of the CRC, in conjunction with provisions sets out in Articles 12 and 17 of the Convention—which protect the right to be heard and the right to have access to information—provides a level of protection of the child's right to freedom of expression.[227] In CRC, freedom of expression has been regarded as having a developmental aspect, since its objective is to enable children to develop themselves in society with others and become participative citizens in public life.[228] Furthermore, according to the Committee on the Rights of the Child, Article 13 of the CRC can be exercised not only against the State but also within the family, in the community, at school, in public policy decisions and in society.[229]

---

220 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 4, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

221 *Report SR 2014 Electoral Processes*, para. 10, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/071/50/PDF/G1407150.pdf?OpenElement>.

222 Ibid.

223 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 95, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

224 "Resolution Adopted by the General Assembly 1386 (XIV). Declaration of the Rights of the Child A/RES/14/1386", 1959, available at <http://www.un-documents.net/a14r1386.htm>.

225 "Special Rapporteur Report on the Right of the Child to Freedom of Expression", para. 10, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf?OpenElement>, accessed 28 May 2015

226 See also Article 7 of the African Charter on the Rights and Welfare of the Child, which entered into force in 1999.

227 "Special Rapporteur Report on the Right of the Child to Freedom of Expression", para. 11, accessed 28 May 2015, available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf?OpenElement.

228 Herdís Thorgeirsdottir, (2006) *A Commentary on the United Nations Convention on the Rights of the Child, Article 13: The Right to Freedom of Expression*, Leiden, Boston: Martinus Nijhoff Publishers, available at <http://innopac.library.drexel.edu:2082/search~S2?/tCommentary+on+the+United+Nations+Convention+on+the+Rights+of+the+Child/tcommentary+on+the+united+nations+convention+on+the+rights+of+the+child/1%2C1%2C11%2CB/frameset&FF=tcommentary+on+the+ united+nations+convention+on+the+rights+of+the+child&5%2C%2C11>.

229 Sylvie Langlaude Doné, "On How to Build a Positive Understanding of the Child's Right to Freedom of Expression", (2010) *Human Rights Law Review,* Vol. 10, No. 1, pp. 33-66, available at <http://papers.ssrn.com/abstract=2020732>.

4.2 Freedom of expression in the digital age

It is widely accepted that innovations in ICTs have created new opportunities for individuals to spread information to a wider audience and thus to have a more significant impact on the right to freedom to access and receive information. The invention and worldwide diffusion of the Internet is reshaping global access to information, communication and services.[230] The Internet is an integral part of the daily life of many individuals and has become a central and key medium for an increasing number of individuals to exercise their right to freedom of expression. However, the Internet may also challenge this right, insofar as the legal and regulatory initiatives that have been created to restrict and control the use of the Internet for information and communication may be used to diminish or violate freedom of expression.

Although access to the Internet is not a human right as such, the UN Special Rapporteur on the promotion of freedom of opinion and expression has reiterated that States have a positive obligation to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise the right, which include the Internet.[231] Similarly, the Human Rights Committee has underscored that States Parties should take all necessary steps to promote the independence of new media and guarantee access to it to all individuals.[232] Also, the Special Rapporteur highlighted that both Article 19 of the UDHR and Article 19 of the ICCPR were drafted with forethought to comprise and adapt to future technological developments through which individuals could exercise their right to freedom of expression.[233] He subsequently concluded that therefore, "the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet".[234] Furthermore, the UN Human Rights Council adopted a landmark resolution in 2012 affirming "the same rights that people have offline must also be protected online".[235]

In the digital age, ICTs also have major impacts on information dissemination in terms of shifting the powers of different actors. For instance, since the Internet has become a crucial and cheap medium for communicating news to a global audience, most of the offline media have developed online alternatives, [236] and this is leading to an emergence of "online journalists"—both professionals and "citizen journalists"—who play an increasingly important role in modern society by documenting and communicating news online. [237] In

230 William H. Dutton et al., *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*, Report, 2013, Paris: UNESCO, p. 8, available at <http://webcache.googleusercontent.com/search?q=cache:0k5FFCefPs4J:unesdoc.unesco.org/images/0019/001915/191594e.pdf+&cd=1&hl=en&ct=clnk>.

231 UN General Assembly, Report of the Special Rapporteur to the General Assembly on the Right to Freedom Opinion and Expression Exercised through the Internet, 10 August 2011, UN Doc A/66/90, para. 61, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>.

232 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 15, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

233 Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 16 May 2011, UN Doc. A/HRC/17/27, para. 15, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27>.

234 Ibid., para. 21.

235 OHCHR, Report of the Special Rapporteur to the Human Rights Council on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 29 June 2012, UN Doc. A/HRC/20/L.13, para. 1, available at <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>.

236 Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom, Report, 2014, Paris: UNESCO, p. 11, available at <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

237 Ibid.

relation to such a power shift, the safety of journalists in the online context—e.g. formally recognized journalists, their support staff or others such as citizen journalists, bloggers, social media actors or human rights defenders—is a necessary condition for the freedom of press and expression.[238] Nonetheless, the shift of power towards individuals in regard to information dissemination coincides with increasing concerns over the protection of others' privacy or private sphere when "reporting" or "recording" can happen at any time and anywhere, which may go against the will of the subject or a given law.[239]

Furthermore, the right to freedom of expression can be enhanced or restricted by the increasing mediating role played by Internet intermediaries. Internet intermediaries are defined as "entities that enable the communication of information from one party to another" In 2010, the Organization for Economic Cooperation and Development (OECD) stated in its report that Internet intermediaries bring together or facilitate transactions between third parties on the Internet. "They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties". The range of intermediaries includes entities such as search engines, ISPs, hosting providers, Cloud computing services, online social networks and media houses, which provide for user-generated content such as comments, blogs or citizen-journalism posts.[240]

On the one hand, Internet intermediaries are crucial in facilitating and protecting the rights to free expression and privacy. On the other hand, they can serve as instruments that enable them and/or governments to monitor, regulate and control an individual's online activities and access to information, thus violating people's rights to privacy and freedom of expression.[241] The potential tensions in this are outlined in UNESCO's study *Fostering Freedom Online: the role of Internet intermediaries*.[242]

4.3 The protection mechanisms: a global review

4.3.1 International law framework

The most authoritative concept in relation to freedom of expression is prescribed by Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). The former contains the first and most widely recognized statement on the right to freedom of expression,[243] stating that everyone has the right to freedom of opinion and expression, including freedom to hold opinions without interference and to seek, receive and impact information and ideas through any media and despite the frontiers. Even though the UDHR is not a binding treaty, it is a recommendatory resolution adopted by the UN General Assembly that, due to time and universal acceptance,

238 Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (Foreign Affairs Council meeting, Brussels, 2014), p. 2, available at <http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf>.

239 See the discussion of two related American cases at Nomad, "Privacy Laws and Citizen Journalism: ACORN and Romney's 47% Speech", *Nomadic Politics*, 14 March 2013, available at <http://nomadicpolitics.blogspot.nl/2013/03/privacy-laws-and-citizen-journalism.html>.

240 Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom, Report, 2014, Paris: UNESCO, p. 7, available at <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

241 Ibid.

242 Ibid.

243 Universal Declaration of Human Rights (UDHR), available at <http://www.un.org/en/documents/udhr/>.

has gained the status of customary international law.[244] The latter, in Paragraphs 1 and 2, requires: a) protection of the right to hold opinions without interference; and b) States parties to guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers, respectively. Furthermore, the latter is regarded to embrace the right of access to information held by public bodies. [245]

The UN Human Rights Committee, as a treaty monitoring body for the ICCPR, provided interpretations of Article 19 of the latter in General Comments, with the most authoritative being provided in 2011 in General Comment 34 (UNHRC/GC34).[246, 247] In this General Comment the Committee has elaborated on the meaning of the right to freedom of expression, and required States parties to ICCPR to contemplate the significance for freedom of expression of developments in ICTs, such as the Internet and mobile-based electronic information dissemination systems.[248]

In 1993, the UN Commission on Human Rights had established the mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and in March 2014 the Human Rights Council had extended the office of the Special Rapporteur for a further period of three years.[249] The annual reports and missions identify new trends and clarify the meaning and scope of the right to freedom of expression. The Human Rights Council unanimously adopted in 2012 the landmark *Resolution on the promotion, protection and enjoyment of human rights on the Internet*, stating that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice in accordance with Articles 19 UDHR and ICCPR.[250]

244 See <http://www.article19.org/pages/en/international-guarantee.html>.

245 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 15, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

246 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 11, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

247 ARTICLE 19, "Defending Freedom of Expression and Information", 28 May 2015, p. 6, available at <http://www.article19.org/>.

248 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 15, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

249 In August 2014, David Kaye was appointed as the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. See <http://www.ohchr.org/EN/ISSUES/FREEDOMOPINION/Pages/OpinionIndex.aspx>.

250 See OHCHR, Report of the Special Rapporteur to the Human Rights Council on the Promotion, Protection and Enjoyment of Human Rights on the Internet, 29 June 2012, UN Doc. A/HRC/20/L.13, para. 1, available at <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>.

4.3.2 Regional law framework

European Union and Council of Europe

The protection of fundamental human rights is one of the basic tenets of EU law.[251] Article 2 of the *Treaty of the European Union* (TEU) prescribes that: '…The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect of human rights, including the rights of persons belonging to minorities…' [252]

Article 11 of the Charter of Fundamental Rights of the European Union defines the right to freedom of expression as including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. It also affirms that everyone has the right to freedom of expression and that the freedom and pluralism of the media shall be respected.[253]

Article 11 of the EU Charter corresponds to Article 10 of the European Convention on Human Rights (ECHR). However, the latter does not prevent States from requiring the licensing of broadcasting or television.[254] Other forms of expression, which are entitled to particular protection in a broader sense by the EU Charter—Articles 10, 12 and 13—include: a) freedom of thought, conscience and religion; b) freedom of assembly and of association; and c) freedom of the arts and sciences.[255]

The ECHR guarantees a wide range of human rights to inhabitants of Member States of the Council of Europe. In Article 10 it states that everyone has the right to freedom of expression, including freedom to hold opinions and to receive and impart information and ideas without interference. However, it also states that these freedoms may be subjected to restrictions as prescribed by law and as necessary in a democratic society, such as restrictions for reasons of national security, public order or public health.

The Committee of Ministers of the Council of Europe monitors the execution of judgments, in particular to ensure payment of remedies or compensations awarded by the Court to the applicants in compensation for the damage they have caused.

The Convention established the European Court of Human Rights (ECtHR), which can be used to bring a case by any person who feels his or her rights have been violated under the Convention by a State Party, when all domestic remedies have been exhausted. The ECtHR judged the first case in 1960, De Becker, concerning Article 10 of the ECHR in view of the lifelong prohibition on carrying on the occupations of journalist and author.[256] Then in 1979 the ECtHR delivered the first judgement on freedom of expression and information in a case unequivocally emphasizing the significance of freedom of expression as one of

251 For more details, see <http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_2.1.2.html>.

252 Consolidated Version of the Treaty on European Union, available at <http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_2.1.2.html>.

253 European Union (EU), *Charter of Fundamental Rights of the European Union*, 2000, p. 11, available at <http://webcache.googleusercontent.com/search?q=cache:vXn6b6iiBXQJ:www.europarl.europa.eu/charter/pdf/text_en.pdf+&cd=3&hl=en&ct=clnk>.

254 Ibid., p. 10.

255 Ibid., p. 6.

256 Council of Europe Publishing, "Freedom of Expression in Europe, Case-Law Concerning Article 10 of the European Convention on Human Rights", p. 11.

the essential foundations and conditions of a democracy and for the development of every man.[257]

In 2014, the Council of European Union issued the EU Human Rights Guidelines on Freedom of Expression Online and Offline, which state that freedom of opinion and expression are fundamental rights of every human being,[258] and affirm that such freedoms are crucial for peace, stability, individual dignity and fulfilment as well as essential requirements for democracy, rule of law,, sustainable inclusive development and participation of public affairs. [259] The guidelines also emphasize the importance of these freedoms for the fulfilment and enjoyment of other human rights, such as the freedom of association and assembly, the freedom of thought, religion or belief, and the right to education. [260]

Other regional instruments

The American Convention on Human Rights—Pact of San Jose, Costa Rica—implemented by the Inter-American Court of Human Rights and Inter-American Commission, introduces the right to freedom of thought and expression in Article 13,[261] which in Paragraph 2 states that the exercise of the right shall not be subject to prior censorship but shall be subject to subsequent imposition of liability. According to Article 13, liability should be established by law to the necessary extent to ensure respect for the rights of others and the protection of national security, public order or public health.

The African Charter on Human and Peoples' Rights, implemented by the African Commission on Human and People's Rights, introduces the right to express and disseminate opinions within the law by Article 9 Paragraph 2.[262] The Declaration of Principles on Freedom of Expression in Africa, implemented by the African Commission on Human and People's Rights, reaffirms in its Preamble the right to receive information and the right to free expression, protected by Article 9 of the African Charter on Human and People's Rights. Article 1 of the Declaration guarantees the freedom of expression and information, including "the right to seek, receive and impart information and ideas, either orally, in writing or in print, in the form of art, or through any other form of communication, including across the frontiers".

The Declaration on Principles of Freedom of Expression (OAS) states, in Principle 1, that freedom of expression in all its forms and manifestations is a fundamental and inalienable right of all individuals, as well as an indispensable requirement for the very existence of a democratic society.[263] Furthermore, in Principle 2 it recalls that every person has the right to

257 ECtHR, *Handyside v. The United Kingdom*, Judgment, 7 December 1976, Application No. 5493/72, para. 49. See also ECtHR, *The Sunday Times v. The United Kingdom*, Judgment, 26 April 1979, Application No. 6538/74, 64.

258 Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (Foreign Affairs Council meeting, Brussels, 2014), p. 1, available at <http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf>.

259 Ibid.

260 Ibid.

261 Organization of American States (OAS), *American Convention on Human Rights 'Pact of San Jose, Costa Rica' (B-32)*, 1969, available at <http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm>.

262 Organization of African Unity, *African Charter on Human and Peoples' Rights (Banjul Charter)*, 1981, available at <http://www.achpr.org/instruments/achpr/>.

263 Organization of American States (OAS), Special Rapporteurship for Freedom of Expression, "Declaration of Principles on Freedom of Expression", 2000, available at <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26>.

seek, receive and impart information and opinions freely under terms set forth in Article 13 of the American Convention on Human Rights.

4.3.3 National law framework

All Member States of the European Union have constitutional protections for freedom of opinion and expression, as they have implemented the main provisions of the Treaty on the European Union, the Treaty on the Functioning of the European Union, and the Charter of Fundamental Rights of the European Union. Upon the adoption of the Lisbon Treaty, a number of amendments were made for implementation. The Charter of Fundamental Rights of European Union became legally binding,[264] the Union acceded to the European Convention of Human Rights,[265] and the fundamental rights guaranteed by the ECHR became binding principles of the Union law.[266] Under the European Convention on Human Rights (ECHR), press freedom, like the right to reputation and privacy, is not interpreted as an absolute right but as a qualified right to be balanced with other rights.[267] The majority of countries have constitutional protection from the national laws with the possibility of appeal to the European Court of Human Rights for violations of freedom of expression and other fundamental rights. [268]

In the USA, the protection granted by the First Amendment and the related case law have gradually established one of the world's strongest freedom of expression protection mechanisms, securing a wide range of speeches and speech actions. The mechanism includes several common law exceptions, relating to obscenity,[269] defamation,[270] incitement,[271] incitement to riot or imminent lawless action,[272] fighting words,[273] fraud, speech covered by copyright, and speech integral to criminal conduct. The USA ratified the ICCPR in 1992. After ratification, the ICCPR became the "supreme law of the land" under the Supremacy Clause of the United States Constitution, which gives acceded treaties the status of federal law.[274] The United States must comply with the implementation of the provisions of the treaty just as it would do with any other domestic law, subject to Reservations, Understanding and Declarations (RUDs) entered when it ratified the treaty. [275] Canada acceded to the ICCPR in 1976. Freedom of expression in Canada is guaranteed by Section 2 Paragraph b of the Canadian Charter of Rights and Freedoms, which among various freedoms states that

264 Article 6 Paragraph 1, Treaty of the European Union, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT&from=EN>.
265 Ibid., Article 6 Paragraph 2.
266 Ibid., Article 6 Paragraph 3.
267 UNESCO, World Trends in Freedom of Expression and Media Development: Regional Overview of Western Europe and North America, 2014, Paris: UNESCO, p. 8, available at <http://unesdoc.unesco.org/images/0022/002277/227741e.pdf>.
268 Ibid.
269 Eric Neisser, (1991) *Recapturing the Spirit: Essays on the Bill of Rights at 200*, Lanham: Rowman & Littlefield, p. 68.
270 Donald E. Biederman, (2007) *Law and Business of the Entertainment Industries*, Westport: Greenwood Publishing Group, p. 457.
271 Ibid.
272 Ibid.
273 Eric Neisser, (1991) Recapturing the Spirit: Essays on the Bill of Rights at 200, Lanham: Rowman & Littlefield, p. 68.
274 ACLU, FAQ: The Covenant on Civil & Political Rights (ICCPR), Parliament of Canada, Constitution Act 1982, Part I, The Canadian Charter of Rights and Freedoms, available at <https://www.aclu.org/faq-covenant-civil-political-rights-iccprl>.
275 Ibid.

everyone has the freedom of thought, belief, opinion and expression, including freedom of press and other media of communication.[276]

Most countries in Latin America and the Caribbean provide constitutional guarantees or laws that protect freedom of expression as a fundamental right, though cases of prior censorship have been frequent.[277] Asia and the Pacific have been in the process of aligning with international standards of freedom of expression.[278] A total of 41 countries (93%) in the region have guaranteed freedom of expression in their constitutions, even though there has been a wide range of implementation levels and possibilities for the right to be overridden by other laws.[279] The national constitutions of 47 African countries contain a guarantee of the right to freedom of expression. However, sub-clauses or other pieces of legislation often stipulate limitations based upon concepts/values such as national security, public order, public morality and public health, without providing a more elaborated understanding of these concepts/values. Nevertheless, journalists have increasingly resisted constraints, and citizens have been able to express themselves relatively freely by means of public media, particularly on Internet forums and in radio talk shows.[280]

4.3.4 Limitations and restrictions

The Human Rights Committee interprets protection of free expression broadly to include expressions that may be regarded as deeply offensive,[281] although certain expressions may also be limited accordingly with the provisions of Article 19 (in Paragraph 3) and are required to be limited under Article 20.[282]

At the same time, freedom of expression is not an absolute right and can be limited when conflicting with other equally important human rights and public interests. Paragraph 3 of Article 19 of the ICCPR articulates that '…the exercise of the rights provided for in Paragraph 2 of this article carries with it special duties and responsibilities and provides the restrictions to this right…' These limitations are legitimate if they fall within the narrow conditions defined in the three-part test in Article 19 of the ICCPR, in Paragraph 3.[283] First, the limitation must be provided by a law or regulation with clarity and precision pursuant to the principle of legal certainty.[284] Second, there must be a legitimate aim to limit the right to freedom of expression. The legitimate aims provided in Article 19 Paragraph 3 ICCPR are exclusive and cannot be added to, including: for respect of the rights or reputations of others, or for the protection of national security or of public order, or of public health or

276 Canadian Charter of Rights and Freedoms, available at <http://laws-lois.justice.gc.ca/eng/const/page-15.html>.

277 UNESCO, World Trends in Freedom of Expression and Media Development: Regional Overview of Western Europe and North America, 2014, Paris: UNESCO, p. 8, available at <http://unesdoc.unesco.org/images/0022/002277/227741e.pdf>.

278 Ibid.

279 Ibid.

280 Ibid.

281 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 11, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

282 Ibid.

283 OHCHR, Report of the Special Rapporteur to the Human Rights Council on Key Trends and Challenges to the Right of All Individuals to Seek, Receive and Impart Information and Ideas of All Kinds through the Internet, 16 May 2011, UN Doc. A/HRC/17/27, para. 8, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement>.

284 ARTICLE 19, available at <http://www.article19.org/pages/en/limitations.html>.

morals. Third, any limitation of the right to freedom of expression must be truly necessary for the protection of that legitimate aim.[285]

The right to privacy, family, home, correspondence, honour and reputation is protected under Article 17 of the ICCPR. The Human Rights Committee has indicated that: "This right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons".[286] However, at the same time, the HRC has observed that "as all persons live in society, the protection of privacy is necessarily relative". Thus, it remains a challenge to balance rights to privacy and protection of reputation with the right to freedom of expression. Nevertheless, the measures taken to limit freedom of expression to protect these rights must comply with the conditions laid down in Article 9 of the ICCPR, in Paragraph 3.

Article 19 of the ICCPR, in Paragraph 3, permits restrictions aimed at protecting public order and national security. For instance, the prohibition of unlawful and harmful activity threatening public order would be a permissible ground when complying with the requirements of necessity and proportionality. This prohibition was considered by the Human Rights Committee specifically with regard to its application to counter-terrorism measures such as broad offences of "praising", "glorifying" or "justifying" terrorism.[287]

Respect for "*public morals*" is a permissible justification for restricting the right to freedom of expression and information. The HRC, in General Comment No. 34, recalled the observation made in General Comment No. 22 that: "The concept of morals derives from many social, philosophical and religious traditions; consequently, limitations […] for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition [and] any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination". [288]

In the online context, the following, amongst other specific types of information mentioned by the Special Rapporteur, can be legitimately limited: a) child pornography (to protect the rights of children); b) hate speech (to protect the rights of affected communities); c) defamation (to protect the rights and reputation of others against unwarranted attacks); d) direct and public incitement to commit genocide (to protect the right of others); and e) advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the right of others, such as the right to life). [289] The Rabat Plan of Action[290], developed by the Office of the High Commissioner for Human Rights provides further guidance in terms of preserving expression from potential overreach in regard to limitation of advocacy of hatred that constitutes incitement (See Chapter 6 below).

---

285 Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 16 May 2011, UN Doc. A/HRC/17/27, para. 8, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27>.; see also HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 12, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

286 OHCHR, CCPR General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), 8 April 1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), para. 1, available at <http://www.refworld.org/docid/453883f922.html>, accessed 29 May 2015.

287 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 46, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

288 Ibid., para. 32.

289 For more details, see UN General Assembly, Report of the Special Rapporteur to the General Assembly on the Right to Freedom Opinion and Expression Exercised through the Internet, 10 August 2011, UN Doc A/66/90, paras. 8-13, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>.

290 http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

CHAPTER 5 Transparency, freedom of information and their protection mechanisms

5.1 Freedom of information and transparency: definitions and contexts

Freedom of information (FOI) and transparency are closely related concepts with long traditions in human civilization, which can be interpreted differently, and which cover diverse ideas and practices in various political-societal contexts. This Chapter analyses the two concepts in different contexts, as well as the related legal-political practices, briefly discussing their distinctions. Additionally, in view of their many overlaps, the Chapter provides an overview of the mechanisms employed to protect them against infringements. While the interplay between the concepts of transparency and FOI forms an indispensable part of this Chapter, it is also discussed further in Chapter 6.

5.1.1 Transparency: in contexts

Transparency as a social value has become important to good governance and it has gained symbolic significance across the world. However, its meaning and history are obscure, as well as its consequences.[291] Despite the explosion of transparency literature, there is still no dominant conceptual definition.[292] Nevertheless, a representative view from the Asian Development Bank, for instance, defines 'transparency' as '…the availability of information to the general public and clarity about government rules, regulations and decisions…'[293]

In general, transparency as a doctrine of governance covers a variety of characteristics, including: a) decision-making in accordance to known and clearly established rather than *ad hoc* principles, guidelines, rules, processes and procedures; b) methods of accounting or public reporting that clarify who gains from, and who pays for any public measures; and c) governance that is intelligible and accessible to the general public.[294]

There are multiple strains of ideas to be traced as partial forerunners for the modern concept of transparency, including: a) the notion of administration by publicly-known rules as one of the oldest ideas in political thought; b) the doctrine of good society that social affairs more generally should be conducted with a high degree of frankness, openness and candour; and c) the idea that the social world should be made knowable by methods analogous to those used in the natural sciences.[295] Since the twentieth century, transparency is found reflected in many doctrines of governance. At the international level, transparency doctrines are important in international governance concerning the way that States relate to one another and to inter- or supra-national bodies, including in diplomacy and the execution of arms control and disarmament treaties.[296] For example, the Paris COP21 agreement includes

291 Christopher Hood, "Transparency in Historical Perspective", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, p. 4.
292 Jonathan Klaaren, "The Human Right to Information and Transparency", in Andrea Bianchi and Anne Peters (Eds.), (2013) *Transparency in International Law*, Cambridge Mass: Cambridge University Press, p. 225.
293 Asian Development Bank, "Governance: Sound Development Management", August 1995, p. 11, available at <http://www.adb.org/documents/governance-sound-development-management>.
294 Christopher Hood, "Transparency in Historical Perspective", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, p. 5.
295 Ibid., pp. 5-10.
296 Ibid., pp. 11-13.

a transparency framework intended to prevent misreporting of nationally determined contributions to combating greenhouse gases.[297]

At the national level, three transparency doctrines concern how a State should relate to citizens in the way it makes decisions or keeps accounts: a) the idea of government according to predictable rules; b) the idea of freedom of information (see below) in dealings between citizens and executive government as a dimension of the above general idea, witnessed in Freedom of Information laws and "sunshine" acts of different States; and c) a different strain of ideas called "transparency" related to the EU usage of the term, namely, that government should operate accounting regimes to separate out different kinds of activities, specifically to make it possible to identify who pays and who benefits from particular programmes and measures. Such doctrines are also increasingly developed in business affairs and most recently corporate governance, relating to the way that managers should relate to stockholders and the financial market about how they conduct and record their affairs.[298]

In their present use, the terms 'transparency', 'openness' and 'access to government-held information' are widely used interchangeably, and regarded as remedies for the deficiencies and operations of governments that fall short of their rhetoric.[299] There are also close relations between the notions of 'transparency' and 'FOI', to the point that they too are on occasions used interchangeably. However, it is important to make a clear distinction between 'transparency' and 'FOI'. Conceptually, FOI has been historically linked to access to public documents and information, and some have suggested that such a right to information should not be limited only to information held by a state.[300] In this perspective, access to information about governance is wider than access to information about governments. However, FOI has generally been narrowly conceived in laws as a qualified right to the information held by a state. On the other hand, 'transparency', according to Heald, in present days is intertwined with a range of social values and public goods in both positive and negative ways, in different contexts, i.e. effectiveness, trust, accountability, autonomy, control, confidentiality, privacy, anonymity, fairness and legitimacy,[301] as well as in the context of the values of accountability and participation.[302]

However, the realization of these ends and values may itself necessitate limits on transparency. Scholars have identified three distinct reasons to limit transparency: a) inappropriate varieties of transparency may impose heavy costs in relation to the realization of certain public goods and rights such as effectiveness and privacy; b) all varieties of transparency may impede the social functions of ignorance, in particular ignorance that may preserve social harmony; and c) transparency is not a "free-for-all", in that it should and must

297 United Nations, (2015). Conference of the Parties Paris Agreement, Framework Convention on Climate Change,. FCCC/CP/2015/L.9/Rev.1. https://unfccc.int/resource/docs/2015/cop21/eng/l09r01.pdf

298 Ibid., pp. 13-19.

299 Patrick Birkinshaw, "Transparency as a Human Right", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, p. 48.

300 See Mariya Riekkinen and Markku Suksi, (2015) *Access to Information and Documents as a Human Right*. Turku: Åbo Akademi University. Institute for Human Rights, Turku: Åbo Akademi University. See also UNESCO, (2016), *Finlandia Declaration (World Press Freedom Day, 3 May 2016) Access to Information and Fundamental Freedoms – This Is Your Right!* http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/WPFD/WPFD2016_Finlandia_declaration_3_may_2016.pdf

301 David Heald, "Transparency as an Instrumental Value", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, pp. 61-68.

302 Andrea Bianchi and Anne Peters (Eds.), (2013) *Transparency in International Law*, , p. 225.

not imply immediate or complete satisfaction of everyone's demands for governmental information.[303]

There are overlaps between transparency and FOI in terms of legislation. In order to achieve transparency and openness of government, 'sunshine' laws are passed to ensure the public access to government – not only to official documents, but also drawing on transparency and 'openness' doctrine to include proceedings. For example, in the USA the principal federal laws providing access to government records are the Freedom of Information Act (FOIA) and the Privacy Act, and the main laws providing access to government meetings are the Federal Advisory Committee Act and the Government in the Sunshine Act. In this specific context, FOI law is a component of 'sunshine' law in the governance realm.

Technological advances in the digital age have reduced the costs to achieve transparency for the public sector, the private sector, and governmental bodies. This not only enables more transparency in such institutions, but also enhances the expectation of the public for more information. However, sunlight that is transformed into searchlight can become uncomfortable for other rights, and sunlight that evolves into torchlight may become destructive.[304] The traditional boundaries between the expectation of transparency and other public interests as listed above—i.e. including privacy, accountability, fairness, effectiveness—have to be redefined for their optimization in adapting to new circumstances

5.1.2 Freedom of information in contexts

Freedom of information can be defined briefly as 'access by individuals as a presumptive right to information held by public authorities'.[305] The UN General Assembly, during its first session in Resolution 59(1), in 1946, recognized the notion of FOI—or the right to access information—in an expanded sense, with the Resolution reading: "Freedom of information is a fundamental human right and is the touch stone of all freedoms to which the UN is consecrated".[306] It is further explained in the Resolution that "freedom of information implies the right to gather, transmit and publish news anywhere and everywhere without fetter".[307]

In this particular wording, FOI as a right legitimizes the free flow of information within society. However, in general, this would include receipt of information, and not only the creation and transmission. This indeed is the perspective of the world's first law on these issues, passed in the territory of present day Sweden and Finland in 1766 (see below). Subsequently, laws relevant to the receiver side in as much as this entailed access to information held by public bodies, were recognized as FOI laws.[308] The right to access information is sometimes

303 David Heald, "Transparency as an Instrumental Value", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, pp. 68-70.

304 Ibid., p. 71.

305 Patrick Birkinshaw, "Transparency as a Human Right", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, p. 50.

306 UN General Assembly, "Calling of an International Conference on Freedom of Information Resolution 59(1)", 14 December 1946, available at <http://www.un.org/documents/ga/res/1/ares1.htm>.

307 Ibid.

308 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 8, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

referred to as the 'right to information'[309] or the 'right to know'.[310] The value and scope of FOI will be further illustrated in Section 5.1.3.

UNESCO's 38th General Conference has endorsed a resolution for the proclamation of 28 September as the "International Day for the Universal Access to Information"[311], which reiterated that the right to information is an integral part of the right to freedom of expression, as recognized by Resolution 59 of the United Nations General Assembly adopted in 1946, and defined in Article 19 of the Universal Declaration of Human Rights (1948), and Article 19 of the International Covenant on Civil and Political Rights.

Freedom of information has been interpreted by the Special Rapporteur in his 1998 Annual Report, as a derived right under Article 19, in that "the right to seek, receive and impart information imposes a positive obligation on States to ensure access to information, particularly with regard to information held by governments".[312] While this reinforces the idea that the right to freedom of expression includes the right to access the information held by government,[313] legally speaking, freedom of information is itself also an independent entitlement, deeply rooted in the long tradition of civil law of mandate, or the concept of agency in common law, in that an individual can only implement his or her plans by relying on other persons who can be supervised only imperfectly.

The significance of FOI rests in the potential tendency of public agents to pursue their own objectives to the detriment of the tasks for which they are hired.[314] One effective measure is the transparency duty of the mandated agent to allow access to related information by principals or mandators. The spirit of this doctrine is reflected in modern liberal democracy, in that elected politicians and public bodies shall, acting as the mandatory, be responsible to the public and provide sufficient information for the supervision of the mandate.

For many, 'FOI' and 'transparency' are used interchangeably, or FOI is approached as a specific feature of transparency with reference to access to government information.[315] According to Birkinshaw, the notion of transparency has a much wider meaning in comparison with the concept of FOI, at least in the EU context. He states that "access to information is a component of transparency, and the latter also entails conducting affairs in the open or subjecting these to public scrutiny". This implies keeping observable records of official decisions and activities for subsequent access by others, and making public processes

309 Ibid., p. 3.

310 OHCHR, *Report of the Special Rapporteur to the General Assembly on the Right to Access Information*, 4 September 2013, UN Doc. A/HRC/68/362, para. 20, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/464/76/PDF/N1346476.pdf?OpenElement>.

311 UNESCO resolution on "International Day for the Universal Access to Information http://unesdoc.unesco.org/images/0023/002352/235297e.pdf

312 United Nations Economic and Social Council (ECOSOC), *Promotion and Protection of the Right to Freedom of Opinion and Expression, Report of the Special Rapporteur, Mr. Abid Hussain*, 28 January 1998, UN Doc. E/CN.4/1998/40, available at <http://www.unhchr.ch/Huridocda/Huridoca.nsf/0/7599319f02ece82dc12566080045b296?Opendocument>.

313 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 8, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

314 Ejan Mackaay, "The Law and Economics of the Civil Law of Mandate", in (2007) *Présentation à La Annual Law & Economics Conference 2007*, Université de Bologne, p. 2, available at <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/727>.

315 Patrick Birkinshaw, "Transparency as a Human Right", in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, p. 47.

and law-making as accessible and comprehensible as possible, so that the involvement of interested parties is enabled as much as possible.[316]

In this sense, the notion of 'transparency' is close to that of 'openness', where the latter covers such items as opening up the processes and meetings of public bodies.[317] The notion of 'openness' however, has a wider scope, such as in the UNESCO concept of Internet Universality where it designates technical interoperability, Net Neutrality, Open Access knowledge principles and opportunities for new entrants (as distinct from closed or monopolized environments).[318] Unlike FOI, transparency has, generally, not been recognized as a human right in international law. Nonetheless over the last decade it has become a frequently used word in both international law scholarship and practice.[319] By contrast, the recognition of FOI as a fundamental human right can be well observed in the global trend towards recognizing the right to information and its importance by authoritative international organizations including the United Nations (UN), the Commonwealth of Nations, Organization of American States (OAS), Council of Europe (COE) and African Union (AU), as well as the popular protection of the right by national FOI laws across the world in recent years.[320]

The origin of freedom of information law can be traced back to Sweden in the 18th century.[321] Colombia also has a long history of freedom of information legislation that dates back to the 1888 Code of Political and Municipal Organization, which allowed individuals to request documents held by government bodies or in government archives. [322] The USA passed its Freedom of Information Law in 1976,[323] followed by other countries. Overall, while only 13 countries had adopted FOI laws by 1990,[324] about 100 countries had done so by 2006.[325] By 2016, this number had risen to 112.[326]

Meanwhile, transparency has been recognized by multilateral development banks and various international financial institutions. For instance, the World Bank and all other four

316 Patrick Birkinshaw, (2010) *Freedom of Information: The Law, the Practice and the Ideal*, Fourth Edition, Cambridge, New York: Cambridge University Press, p. 29.

317 Andrea Bianchi and Anne Peters (Eds.), (2013) *Transparency in International Law,* pp. 29-31.

318 http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/internet-universality/

319 Transparency is even not immediately associated with international law according to Andrea Bianchi. Andrea Bianchi, (2013) *On Power and Illusion: the Concept of Transparency in International Law*, Cambridge: Cambridge University Press, see Ibid., p. 3.

320 See Toby Mendel, (2003) *Freedom of Information: A Comparative Legal Survey*,, Paris: UNESCO, p. 19, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-information-a-comparative-legal-survey/>.

321 *The World's First Freedom of Information Act, Anders Chydenius' Legacy Today*, Publications 2 (Kokkola: Anders Chydenius Foundation, 2006), p. 4, available at <http://webcache.googleusercontent.com/search?q=cache:bxxyVLf5aZsJ:www.chydenius.net/pdf/worlds_first_foia.pdf+&cd=1&hl=en&ct=clnk>.

322 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 22, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

323 USC Title 5, Section 552.

324 See ARTICLE 19, available at <http://www.article19.org/resources.php/resource/3024/en/international-standards:-right-to-information#_ftn16>; see also David Banisar, "Freedom of Information Around the World 2006: A Global Survey of Access to Government Information Laws", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 20 September 2006), Appendix A, available at <http://papers.ssrn.com/abstract=1707336>.

325 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 3, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

326 See Global Right To Information Rating: <http://www.rti-rating.org/>.

regional development banks have adopted information disclosure policies.[327] UN bodies are also adopting access to information policies, and initiatives like the Carbon Disclosure Project have enlisted large companies to report on their environmental impact.

Combined with these initiatives, overall it is safe to say that 'there has been a veritable revolution in recent years in terms of the right to information'[328] In these developments, it is worth noticing the shift in the terminology used when referring to FOI. While in the past the most commonly used term was 'freedom of information', nowadays the term '*right to information*' is gaining popularity amongst both civil society actors and officials; e.g. as reflected in the title of the 2005 India law granting access to information held by public authorities.[329] While the right to information has a logical link to the notion of access to information, the latter has a wider scope that covers enabling conditions, and extending into issues of accessibility, as outlined in the UNESCO 2015 Study Keystones to foster inclusive Knowledge Societies.[330]

5.1.3 The value and scope of freedom of information

FOI is indispensable to, *inter alia*, fostering citizens' effective participation, building trust in government, reducing corruption, and enabling the realization of other human rights. This view coincides with six other views. First, that FOI is crucial to democratic states and good governance. This is based on the ideas that: information must be accessible to members of the public in the absence of an overriding public interest in secrecy;[331] that the public has the right to scrutinize the actions of their politicians and to engage in open and full debate about those actions to promote good governance;[332] and that citizens more specifically must have access to public information related to State activity to achieve effectiveness in democratic procedures.[333] Second, that freedom of information is crucial for the development of individuals,[334] since it assures their autonomy and self-fulfilment[335] and allows them to pursue and search for truth and the advance of knowledge.[336] Third, that journalists and actors in civil society play a critical role by using the right to access

327 Including the Inter-American Development Bank, the African Development Bank Group, the Asian Development Bank, the European Bank for Reconstruction and Development.

328 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 3, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

329 Ibid.

330 http://www.unesco.org/new/en/internetstudy

331 OHCHR, *Report of the Special Rapporteur to the General Assembly on the Right to Access Information*, 4 September 2013, UN Doc. A/HRC/68/362, para. 20, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/464/76/PDF/N1346476.pdf?OpenElement>.

332 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 4, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

333 OHCHR, Report of the Special Rapporteur to the Human Rights Council on Limitations to the Right to Freedom of Expression, Safety and Protection of Journalists and Media Professionals in Conflict Zones, and Right of Access to Information in Situations of Extreme Poverty, 30 April 30 2009, UN Doc. A/HRC/11/04, para. 31, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/11/4>.

334 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 1, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

335 Thomas I. Emerson, (1970) *The System of Freedom of Expression*, New York: Random House Trade Paperbacks, p. 6. See also UNESCO, (2013) *Freedom of Expression Toolkit: A Guide for Students*, Paris: UNESCO, p. 13, available at <http://unesdoc.unesco.org/images/0021/002186/218618E.pdf>.

336 UNESCO, (2013) *Freedom of Expression Toolkit: A Guide for Students*, Paris: UNESCO, p. 13, available at <http://unesdoc.unesco.org/images/0021/002186/218618E.pdf>.

information to expose wrongdoings and help with finding remedies.[337] Fourth, that the right to information is used to facilitate effective business practices. Public bodies have important information relating to economic matters that can be useful for businesses, therefore the right to information facilitates the promotion of information flows between government and the business sector.[338] Fifth, that the right to access information is crucial for the realization of other human rights. It is an intrinsic part of the full exercise of the right to freedom of expression.[339]

Furthermore, a particular dimension of the right to seek and receive information concerns access to information on human rights violations, insofar as such access often determines the degree of enjoyment of other rights.[340] Furthermore, the right of access to one's personal information is part of the fundamental value of human dignity. For instance, access to medical records can help individuals make decisions on treatment and financial planning and, therefore, access to one's personal information will facilitate effective personal decision-making. Nevertheless, in line with Heald's views, the relationship between transparency and other values may not always be positive,[341] as evident from the conflicts that may exist between transparency and information privacy.

The right to access information is widely seen today as encompassing both the right to access information held by public bodies, as well as the right of citizens and media actors to access information by other actors and which is of public interest or which is information concerning them that can affect their rights.[342]. With regard to Article 17 of the ICCPR, the Human Rights Committee has observed that every individual should also be able to ascertain which public authorities or private individuals or bodies control his or her files, and for what purposes.[343] Moreover, every individual should also be able to know which public authorities or private individuals or bodies control or may control his or her files.[344] Furthermore, if such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to have his or her records rectified.[345] These latter rights of access and rectification, have been of course, also closely related to privacy and data protection law especially in the sphere of those European countries which have adopted such principles as part of their transposing into their national laws the Council of Europe's 1981 Convention 108.

---

337 OHCHR, *Report of the Special Rapporteur to the General Assembly on the Right to Access Information*, 4 September 2013, UN Doc. A/HRC/68/362, para. 69, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/464/76/PDF/N1346476.pdf?OpenElement>. See also Maeve McDonagh, "The Right to Information in International Human Rights Law", (2013) *Human Rights Law Review*, Vol. 13, No. 1, p. 4, available at <http://papers.ssrn.com/abstract=2446424>.

338 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 4, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

339 OHCHR, *Report of the Special Rapporteur to the General Assembly on the Right to Access Information*, 4 September 2013, UN Doc. A/HRC/68/362, para. 4, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/464/76/PDF/N1346476.pdf?OpenElement>.

340 Ibid., para. 9.

341 Jonathan Klaaren, "The Human Right to Information and Transparency", in Andrea Bianchi and Anne Peters (Eds.), (2013) *Transparency in International Law*, Cambridge Mass: Cambridge University Press, p. 225.

342 OHCHR, *Report of the Special Rapporteur to the General Assembly on the Right to Access Information*, 4 September 2013, UN Doc. A/HRC/68/362, para. 19, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/464/76/PDF/N1346476.pdf?OpenElement>.

343 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 18, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

344 Ibid.

345 Ibid.

The definition of 'information' varies in different jurisdictions.[346] In most circumstances, laws define information in broad terms to comprise all forms in which content may be recorded, such as in written form, in electronic form, or in other storage systems. [347] The right to access information, as is often taken to be implied by UDHR and ICCPR, includes records held by a public body, regardless of the form,[348] in which the information is stored, its source or the date of production.[349] Such right comprises information from political discourse,[350] commentary on one's own[351] and on public affairs,[352] canvassing,[353] discussion of human rights,[354] journalism,[355] cultural and artistic expression,[356] teaching,[357] and religious discourse;[358] and it may also include commercial advertising. Generally, the right to access information applies to all information regardless of the purpose for which it is held, though some laws may restrict the scope of the 'information', for instance in regard to information held for official purposes that merit exemption from access.[359]

The ICCPR is binding on every State Party as a whole. [360] All branches of the State and other public or government authorities at any level—i.e. national, regional or local—are in a position to exercise the responsibility of the State Party.[361] Such responsibility may also be incurred by a State Party under certain circumstances with respect to acts of semi-State entities.[362] The designation of such bodies may also include other entities when carrying out public functions.[363] Moreover, the obligation requires State Parties to guarantee individuals' protection from any acts by private persons or entities that would undermine the enjoyment

346 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 142, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

347 Ibid.

348 "[…] either orally, in writing or in print, in the form of art, or through any other media of his choice […]" (Article 19 ICCPR).

349 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 18, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

350 HRC, *Essono Mika Miha v. Equatorial Guinea*, Communication No. 414/1990, UN Doc. CCPR/C/51/D/414/1990.

351 HRC, *Anthony Fernando v. Sri Lanka*, Communication No. 1189/2003, UN Doc. CCPR/C/83/D/1189/2003 (2005).

352 HRC, *Patrick Coleman v. Australia*, Communication No. 1157/2003, UN Doc. CCPR/C/87/D/1157/2003 (2006).

353 "Concluding Observations on Japan (CCPR/C/JPM/CO/5)", available at <http://www.nichibenren.or.jp/library/ja/kokusai/humanrights_library/treaty/data/CO_JPRep6_ICCPR140820.pdf>, accessed 23 August 2015.

354 HRC, *Mr. Vladimir Velichkin v. Belarus*, Communication No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

355 HRC, *Mavlonov and Sa'di v. Uzbekistan*, Communication No. 1334/2004, UN Doc. CCPR/C/95/D/1334/2004 (2009).

356 HRC, *Hak-Chul Shin v. Republic of Korea*, Communication No. 926/2000, UN Doc. CCPR/C/80/D/926/2000 (2004).

357 HRC, *Ross v. Canada*, Communication No 736/1997, UN Doc. CCPR/C/70/D/736/1997 (2000).

358 See HRC, *Hak-Chul Shin v. Republic of Korea*, Communication No. 926/2000, UN Doc. CCPR/C/80/D/926/2000 (2004).

359 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 142, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

360 See HRC, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 4, available at <https://www1.umn.edu/humanrts/gencomm/hrcom31.html>.

361 Ibid.

362 See HRC, Leo Herzberg et al v. Finland, Communication No. 16/1979, UN Doc. CCPR/C/OP/1 at 124 (1985).

363 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 18, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

of Covenant rights, insofar as they are amenable to application between private persons or entities.[364] Furthermore, State Parties are required to guarantee that the rights contained in Article 19 of the ICCPR are given effect within the domestic law. Additionally, this should be done in a consistent manner and with the guidance provided by the Committee on the nature of the general legal obligation imposed on State Parties to the Covenant.[365]

The Human Rights Committee has further emphasized that in order to give effect to the right to access information, States Parties should place government information of public interest in the public domain, proactively.[366] The Committee stated that States Parties should make efforts to ensure "easy, prompt, effective and practical access to such information".[367] The Special Rapporteur stated, in 2010, that governments should take necessary legislative and administrative measures to improve access to public information for everyone.[368] It also specified that there are specific legislative and procedural characteristics that any policy on the access to information must have, such as: a) the requirement of the observance of the principle of maximum disclosure; b) the presumption of the public nature of meetings and key documents; c) broad definitions of the type of information that is accessible; d) reasonable fees and time limits; e) independent reviews of any refusals to disclose information; and f) sanctions for non-compliance with the policy.[369]

5.1.4 Moving into the digital age

Since late 1990s, the invention and global diffusion of the Internet and ICTs have made great impacts on FOI, transparency and openness. The Internet has gradually become a central, prevailing medium for many individuals to disseminate expression, and to access all kinds of information.[370] Many governments have increasingly used novel ICTs—e.g. social media—as an efficient means to curtail corruption, promote openness and transparency, and improve e-governance and e-democracy.[371] According to the UN Special Rapporteur, "[t]he Internet can primarily be used as a positive tool to increase transparency over the

364 HRC, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 8, available at <https://www1.umn.edu/humanrts/gencomm/hrcom31.html>.; see also HRC, *Robert W. Gauthier v. Canada*, Communication No. 633/1995, UN Doc. CCPR/C/65/D/633/1995 (1999).

365 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 8, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.; see also HRC, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 4, available at <https://www1.umn.edu/humanrts/gencomm/hrcom31.html>.

366 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 19, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

367 Ibid.

368 Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, 20 April 2010, para. 32, available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf>.

369 Ibid., para. 32.

370 William H. Dutton et al., *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*, Report, 2013, Paris: UNESCO, p. 8, available at <http://webcache.googleusercontent.com/search?q=cache:0k5FFCefPs4J:unesdoc.unesco.org/images/0019/001915/191594e.pdf+&cd=1&hl=en&ct=clnk>.

371 John Carlo Bertot, Paul T. Jaeger and Justin M. Grimes, "Promoting Transparency and Accountability through ICTs, Social Media, and Collaborative E-Government", (2012) *Transforming Government: People, Process and Policy,* Vol. 6, No. 1, pp. 2-3, available at <http://www.emeraldinsight.com/doi/full/10.1108/17506161211214831>.

conduct of those in power, access diverse sources of information, facilitate active citizen participation in building democratic societies and counter authoritarian regimes".[372]

With respect to FOI, what has accompanied this big change is the rise of the private sector players, in that they are taking over more and more of the public functionalities that previously belonged exclusively to public bodies in relation to the processing of personal data. Additionally, these private sector players collect and control a large bulk of personal data to which individuals have equally the FOI right, such as when personal privacy and data security are of concern.[373] Such changes are opening a debate on the accountability of the private sector in regard to its impact on human rights.

For instance, in 2000 the United Nations Development Programme (UNDP) contended that the State-centred model of accountability must be extended to the obligations of non-State actors. [374] In the Guiding Principles on Business and Human Rights endorsed by the Human Rights Council in 2011, it is explained that while governments have a primary duty to protect human rights, companies have a responsibility to respect these rights, and both governments and companies should provide access to effective remedy. Guidance is also given for companies to fulfil these norms. In this evolving context, the developments in the storage and processing of public information have increasingly allowed the FOI laws to cover information and data that is held—even if only partially—by the private sector. In this way, the right to seek and receive information is a cornerstone for data protection regimes and their role in protecting the right to privacy. With the rise of "big data" and algorithms that process huge samples, new issues arise as to the extent to which access to "information" includes access to "data", "metadata" and algorithms that convert data into information.

5.2 Transparency and freedom of information protection mechanisms

5.2.1 International frameworks

Article 19 of the UDHR provided the first and most widely recognized statement of the right to freedom of expression, including the right to seek and receive information. Additionally, Article 19 of the ICCPR guarantees the right to freedom of opinion and expression, also including reference to the right to seek and receive information within the broader expression right. In 1993, the UN Commission on Human Rights established the Office of the UN Special Rapporteur on freedom of opinion and expression, and called on the Special Rapporteur to "develop further his commentary on the right to seek and receive information and to expand on his observations and recommendations arising from communications".[375] Fulfilling these obligations, the Special Rapporteur's report issued in 1998 referred to Article 19 as imposing "a positive obligation on states to ensure access

372 UN General Assembly, Report of the Special Rapporteur to the General Assembly on the Right to Freedom Opinion and Expression Exercised through the Internet, 10 August 2011, UN Doc A/66/90, para. 12, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>.

373 The Court has recently moved towards a broader interpretation of the notion of freedom to receive information and thereby towards the recognition of a right to information. ECtHR, *Társaság a Szabadágjogokért v. Hungary*, Judgment, 14 April 2009, Application No. 37374/05, para. 35.

374 Mazhar Siraj, "Exclusion of Private Sector from Freedom of Information Laws: Implications from a Human Rights Perspective", (2010) *Journal of Alternative Perspectives in the Social Sciences*, Vol. 2, No. 1, p. 215.

375 OHCHR, "Right to Freedom of Opinion and Expression", 11 April 1997, C.H.R. Res. 1997/27, ESCOR Supp. (No. 3) at 100, UN Doc. E/CN.4/1997/27, para. 12(d), available at <http://www.unhchr.ch/Huridocda/Huridoca.nsf/TestFrame/3b49a725e6586472802566430059 69e6?Opendocument>.

to information, particularly with regard to information held by governments",[376] which view is reinforced by a report issued in 2005.[377] The 2000 Special Rapporteur's report on Freedom of Opinion and Expression pointed out the fundamental importance of the FOI for both freedom and democracy; and the right to participate and to realization of the right to development.[378] In the 2000 report, the Rapporteur also reiterated concern about "the tendency of Governments, and the institutions of Government, to withhold from the people information that is rightly theirs".[379] Further, he elaborated on the specific content of the right to information. [380] In 2004, the UN Special Rapporteur on Freedom of Opinion and Expression co-issued a joint declaration with other rapporteurs, recognizing the right to access information as a fundamental human right based on the principle of maximum disclosure.[381] Moreover, in 2010, UNESCO marked the World Press Freedom Day by issuing the Brisbane Declaration, which called on national governments that had not already adopted access to information laws to do so "based on international standards and the principle of maximum disclosure".[382] The Finlandia Declaration at the UNESCO World Press Freedom Day conference in 2016, amplifies these messages.[383]

The UN Human Rights Committee (HRC) reviews and comments on the regular reports that States provide to the HRC to implement the ICCPR obligations. It also hears individual complaints about human rights violations from States that have ratified the First Optional Protocol to the ICCPR.[384] In 2011, the HRC published General Comment No. 34 with an authoritative interpretation of the freedom of opinion and expression guaranteed by Article 19 of the ICCPR, expressly acknowledging that Article 19 of the ICCPR embraces a general right of access to information held by public bodies. Moreover, General Comment No. 34 noted that Article 19 of the ICCPR, in conjunction with Article 25 of the ICCPR, had previously been interpreted by the Committee as including a right to media to access to information

376 UN General Assembly, Report of the Special Rapporteur to the General Assembly on the Right to Freedom Opinion and Expression Exercised through the Internet, 10 August 2011, UN Doc A/66/90, para. 61, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>.

377 OHCHR, Report of the Special Rapporteur on Implementing the Right of Access to Information and Protection and Security of Media Professionals, 17 December 2004, UN Doc. E/CN.4/2005/64, para. 39, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G05/106/90/PDF/G0510690.pdf?OpenElement>; see also OHCHR, Report of the Special Rapporteur to the Human Rights Council on Limitations to the Right to Freedom of Expression, Safety and Protection of Journalists and Media Professionals in Conflict Zones, and Right of Access to Information in Situations of Extreme Poverty, 30 April 2009, UN Doc. A/HRC/11/04, para. 60, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/11/4>.

378 OHCHR, Report of the Special Rapporteur on Access to Information, Criminal Libel and Defamation, the Police and the Criminal Justice System, and New Technologies, 18 January 2000, UN Doc. E/CN.4/2000/63, para. 42, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G00/102/59/PDF/G0010259.pdf?OpenElement>.

379 Ibid., para. 43.

380 Ibid., para. 44.

381 OSCE, "Joint Declaration on Freedom of Expression and the Internet (OSCE, UN, OAS and ACHPR)", 1 June 2011, available at <http://www.osce.org/fom/78309>.

382 UNESCO, Brisbane Declaration: Freedom of Information, The Right to Know, 3 May 2010. "Brisbane Declaration, Freedom of Information: The Right to Know" (UNESCO World Press Freedom Day conference, Brisbane, Australia, 2010), available at <http://www.unesco.org/new/en/unesco/events/prizes-and-celebrations/celebrations/international-days/world-press-freedom-day/previous-celebrations/2010/brisbane-declaration/>.

383 http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/WPFD/WPFD2016_Finlandia_declaration_3_may_2016.pdf

384 First Optional Protocol to the ICCPR, available at <http://www.ohchr.org/EN/HRBodies/TBPetitions/Pages/HRTBPetitions.aspx>.

on public affairs[385] and the right of the general public to receive media output.[386] Also, General Comment No. 34 further states that in order to give effect to the right of access to information, States Parties should put in the public domain government information of public interest, proactively.[387]

Furthermore, the HRC referred to General Comment No. 16 regarding Article 17 ICCPR, addressing the right to privacy, which addresses access to, and amendment of personal data relating to individuals.[388] The HRC also observed that General Comment No. 32 regarding Article 14 of the ICCPR, addressing the right to a fair trial, sets out the various entitlements to information that are held by those accused of a criminal offence.[389] The HRC further referred to the fact that Article 10 of the ICCPR, addressing the right to liberty, had been interpreted by the Committee as preserving the right of prisoners to access medical records.[390] Finally, the HRC noted that, as observed in General Comment No. 31, persons should be in receipt of information regarding their Covenant rights according to Article 2 of the Covenant.[391]

In 1998, the UN Economic Commission for Europe adopted the Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters. The Convention establishes a number of rights of the public with regard to the environment,[392] including the right of everyone to receive environmental information held by public authorities, which can include information on the state of the environment and on policies or measures taken, or on the state of human health and safety where this can be affected by the state of the environment. [393] In Article 13 of ZZ, the Convention against Corruption, which was adopted by the General Assembly Resolution 58/4 in 2003,[394] prescribed that participation should be strengthened by measures such as ensuring that the public has effective access to information.[395]

385 HRC, *Robert W. Gauthier v. Canada*, Communication No. 633/1995, UN Doc. CCPR/C/65/D/633/1995 (1999).

386 HRC, *Mavlonov and Sa'di v. Uzbekistan*, Communication No. 1334/2004, UN Doc. CCPR/C/95/D/1334/2004 (2009).

387 HRC, CCPR General Comment No. 34: Article 19 (Freedoms of Opinion and Expression), 12 September 2011, UN Doc. CCPR/C/GC/34, para. 19, available at <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

388 OHCHR, CCPR General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), 8 April 1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), available at <http://www.refworld.org/docid/453883f922.html>, accessed 29 May 2015.

389 HRC, General Comment No. 32: Article 14, Right to Equality before Courts and Tribunals and to Fair Trial", 23 August 2007, UN Doc. CPPR/C/GC/32, available at <http://www.refworld.org/docid/478b2b2f2.html>.

390 HRC, *Mrs. Tatiana Zheludkova v. Ukraine*, Communication No. 726/1996, UN Doc. CCPR/C/75/D/726/1996 (2002**).**

391 HRC, General Comment No. 31 on the Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, paras. 3-5, available at <https://www1.umn.edu/humanrts/gencomm/hrcom31.html>.

392 EU, Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention), 1998, available at <http://ec.europa.eu/environment/aarhus/>.

393 Ibid.

394 UN General Assembly, United Nations Convention against Corruption, 31 October 2003, UN Doc. A/RES/58/4, available at <http://www.un-documents.net/a58r4.htm>.

395 Ibid.

5.2.2 Regional framework

Council of Europe

Article 10 of the European Convention on Human Rights (ECHR), implemented by the European Court of Human Rights, prescribes that everyone has the right to freedom of expression, which includes "freedom […] to receive […] information and ideas without interference".[396] In 2008, the Convention on Access to Official Documents and its Explanatory Report were adopted. This first multilateral treaty affirms and articulates an enforceable general right to information that can be exercised by all persons without demonstrating a particular interest in the information requested.[397] This treaty came a full generation after the Committee of Ministers of the Council of Europe adopted Recommendation No. R (81) 19 on the Access to Information Held by Public Authorities, prescribing that everyone under the jurisdiction of a Member State shall have the right to information held by public authorities other than legislative bodies and judicial authorities.[398]

The Recommendation Rec (2002) 2 on Access to Official Documents includes general principles on access to official documents.[399] It recommends that Member States guarantee the right of everyone to have access, upon request, to official documents held by public authorities, and highlights that such principle should apply without discrimination on any ground, including national origin.[400] In 2014, the Council of the European Union issued the EU Human Rights Guidelines on Freedom of Expression Online and Offline to promote and protect freedom of opinion and expression, which state that ensuring access to information can serve to promote justice and reparation, particularly after periods of grave violations of human rights.[401]

European Union

Article 42 of the Charter of Fundamental Rights of the European Union and Article 15 of the Treaty on the Functioning of the European Union (TFEU) give "any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, […] a right of access to documents of the institutions, bodies, offices and agencies of the Union, whatever their medium". It follows from Article 15 of the TFEU, in that the right is "subject to the principles and the conditions to be defined" in legislation.[402] In 2003, the European Parliament and the European Council adopted Directive 2003/98/EC on the re-use of public sector information, which sets out the rules and practices for accessing public sector

396 See also ECtHR, *Guerra and others v. Italy*, Judgment, 19 February 1998, Application No. 14967/89.
397 EU, Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention).
398 Recommendation No.R (81)19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities, Council of Europe, Committee of Ministers, 25 November 1981, 2, available at <http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec%281981%29019_EN.asp>.
399 Recommendation Rec(2002)2 of the Committee of Ministers to Member States on Access to Official Documents, Council of Europe, Committee of Ministers, 21 February 2002, 2, available at <https://wcd.coe.int/ViewDoc.jsp?id=262135>.
400 Ibid.
401 Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (Foreign Affairs Council meeting, Brussels, 2014), p. 3, available at <http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf>.
402 EU, Charter of Fundamental Rights of the European Union.

information resources for further exploitation.[403] In 2001, Regulation (EC) No 1049/2001 regarding Public Access to European Parliament, Council and Commission Documents defined the right of access to documents of the three institutions. This regulation also applies to the majority of other EU bodies and agencies, when there is no provision in their establishing legal acts.[404]

The Commonwealth of Nations

In 1980, the Law Ministers of the Commonwealth stated that: "public participation in the democratic and governmental process was at its most meaningful when citizens had adequate access to official information".[405]In 1991, the Commonwealth adopted the Harare Commonwealth Declaration and ensured each individual's democratic right to participate in framing his or her society.[406] The Commonwealth has subsequently taken a number of important steps to further expand the content of that right. In 1999, the Commonwealth Secretariat created a Commonwealth Expert Group to discuss the right to information, which adopted a document establishing a number of principles and guidelines on freedom of information,[407] which were supported by the Commonwealth Law Ministers at the 1999 meeting in Port of Spain, Trinidad and Tobago.[408]

After considering the Law Ministers' communiqué, the Committee of the Whole on Commonwealth Functional Cooperation issued a report, approved later by the Heads of Government, in which they expressed their recognition of the importance of public access to official information, both in promoting transparent and accountable governance and in encouraging full participation of citizens in democratic process.[409] The Commonwealth Secretariat took steps to promote the right to information in member countries, such as by drafting model laws on the right to information and on privacy.[410]

---

403 Directive on the re-use of public sector information, see 2003/98/EC European Union (EU), Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-Use of Public Sector Information, vol. L 345/90, 2003, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:en:PDF>.

404 EU, *Regulation (EC) No 1049/2001 Regarding Public Access to European Parliament, Council and Commission Documents*, 2001, available at <http://webcache.googleusercontent.com/search?q=cache:vjgb_-4_QNwJ:www.europarl.europa.eu/RegData/PDF/r1049_en.pdf+&cd=2&hl=en&ct=clnk>.

405 Quoted in "Promoting Open Government: Commonwealth Principles and Guidelines on the Right to Know" (Commonwealth Expert Group Meeting on the Right to Know and the Promotion of Democracy and Development, London, 1999), available at <http://www.humanrightsinitiative.org/programs/ai/rti/international/cw_standards/commonwealth_expert_grp_on_the_rti_99-03-00.pdf>.

406 Commonwealth Heads of Government Meeting, 20 October 1991, paras. 4 and 9. Heads of Government in Harare, "Harare Commonwealth Declaration" (Harare, Zimbabwe: The Commonwealth, 1991), paras. 4 and 9, available at <http://thecommonwealth.org/history-of-the-commonwealth/harare-commonwealth-declaration>. See also The Common Wealth, "Millbrook Commonwealth Action Plan on the Harare Declaration" (London, 12 November 1995), available at <http://thecommonwealth.org/history-of-the-commonwealth/millbrook-commonwealth-action-plan-harare-declaration>.

407 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, pp. 12-13, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

408 "1999 Meeting of Commonwealth Law Ministers and Senior Officials", Vol. 2 (Port of Spain, Trinidad and Tobago, 3-7 May), available at <http://www.oecd-ilibrary.org/commonwealth/governance/1999-meeting-of-commonwealth-law-ministers-and-senior-officials_9781848597624-en>.

409 Communiqué, Commonwealth Functional Cooperation Report of the Committee of the Whole (Durban: Commonwealth Heads of Government Meeting, 15 November 1999), para. 20.

410 The Freedom of Information Act, available at <http://www.humanrightsinitiative.org/programs/ai/rti/international/cw_standards/Cth%20model%20law%20-%20FOI%20Act.pdf>; see also Privacy Act, available at <http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7B82BDA409-2C88-4AB5-9E32-797FE623DFB8%7D_protection%20of%20privacy.pdf>.

The African Region

Article 9 of The African Charter on Human and People's Rights, which was adopted in 1981, provides that every individual shall have the right to receive information.[411] The African Charter on Democracy, Elections and Good Governance was adopted by the African Union in 2007. Article 2 of the Charter emphasizes the importance to promote the establishment of the necessary conditions to foster citizen participation, transparency, access to information, freedom of the press, as well as accountability in the management of public affairs. Article 19 provides that in electoral processes each State Party shall guarantee conditions of security, free access to information, non-interference, freedom of movement and full cooperation with the electoral observer mission.[412]

Article 6 of the African Charter on Values and Principles of Public Service and Administration protects the right of access to information held by public service and administration regarding procedures and formalities pertaining to public service delivery.[413] Article 9 of the African Convention on Preventing and Combating Corruption demands that each party adopts legislative and other measures to give effect to the right of access to any information required to fight against corruption and related offences. [414] Article 1 of The Declaration of Principles on Freedom of Expression in Africa states that freedom of expression and information—which includes the right to seek, receive and impart ideas—is a fundamental and inalienable human right and an indispensable component of democracy.[415] The Model Law on Access to Information for Africa provides specific guidelines of forms and contents of such legislation.[416]

The American Region

Adopted in 1969, the American Convention on Human Rights (Pact of San José) is implemented by the Inter-American Court of Human Rights and Inter-American Commission. Article 13 of the Convention protects the right to freedom of thought and expression.[417] The General Assembly resolution AG/RES. 2516 of the Organization of American States (OAS) demanded the preparation of The Model Inter-American Law on Access to Information.[418] It provides Member States with the legal foundation to guarantee the right to access to information. The Implementation Guide for the Model Law provides a roadmap to ensure

411 Organization of African Unity, African Charter on Human and Peoples' Rights (Banjul Charter).

412 African Union (AU), African Charter on Democracy, Elections and Governance, 2007, available at <http://webcache.googleusercontent.com/search?q=cache:67DX2NO2UXwJ:www.ipu.org/idd-E/afr_charter.pdf+&cd=1&hl=en&ct=clnk>.

413 African Union (AU), African Charter on Values and Principles of Public Service and Administration, 2011, available at <http://www.au.int/en/content/african-charter-values-and-principles-public-service-and-administration>.

414 African Union (AU), Convention on Preventing and Combating Corruption, 2003, available at <http://www.au.int/en/sites/default/files/AFRICAN_UNION_CONVENTION_PREVENTING_COMBATING_CORRUPTION.pdf>.

415 African Commission on Human and Peoples' Rights, "Declaration of Principles on Freedom of Expression in Africa", 17 October 2002, available at <http://www1.umn.edu/humanrts/achpr/expressionfreedomdec.html>.

416 See <http://www.article19.org/resources.php/resource/3642/en/gambia:-african-commission-adopts-model-law-on-access-to-information>.

417 Organization of American States (OAS), American Convention on Human Rights "Pact of San Jose, Costa Rica" (B-32).

418 OAS, "Model Inter-American Law on Access to Information, A/RES/2514 (XXXIX-O/09)", 8 June 2010, available at <http://www.oas.org/en/sla/dil/access_to_information_model_law.asp>.

that the law may function in practice.[419] The model law incorporates the principles outlined by the Inter-American Court on Human Rights in Claude Reyes v. Chile, and the Principles on Access to Information adopted by the Inter-American Juridical Committee.[420] Principle 2 recalls that every person has the right to seek, receive and impart information and opinions freely under terms set forth by Article 13 of the American Convention on Human Rights.[421] The OAS also adopted the Resolution on Access to Public Information: Strengthening Democracy in 2009.[422]

5.2.3 National law framework

National laws vary with respect to the rules to be adopted in processing requests for information. In general, all laws require that such requests be made in writing, or electronically, including the name and contact details of the applicant, and a detailed description of the information sought for identification.[423] Whilst most countries do not require the provision of a reason upon request, others, such as Sweden, request the provision of additional information for the processing of the application, including the reason for the applicant's request.[424] Most laws provide special provisions to assist applicants when they encounter difficulties; for instance, when a written request is not possible due to illiteracy or disability.[425]

Nearly all laws provide time limits for responses to requests for information, which range from 7 to 30 days. Additionally, most laws require the information to be provided as soon as possible within a maximum period,[426] allowing for an extension in case of, for instance, a complicated search through a record not located at the main office, or the need of consultations with others. [427] Furthermore, nearly all laws require public bodies to give written notice of responses to requests of information. For a granted request, such a notice may include any fees and the form in which the request is to be granted. For a refused request, the notice normally includes the grounds of refusal, along with information about the right to appeal against the refusal,[428] which allows the requester to decide whether or not to follow any appeal options. [429]

Moreover, many countries allow applicants to select from a range of forms of access, including: personal inspection of the document in question, transcripts, electronic copies, photocopies, and official copies. It is complex to determine the extent of the efforts that public bodies should be required to make to present information in a form in which it is

419 Ibid.
420 OAS, "Principles on the Right of Access to Information CJI/RES.147 (LXXIII-O/08)", 7 August 2008, available at <http://webcache.googleusercontent.com/search?q=cache:FroG00C8QK0J:www.oas.org/cji/eng/CJI-RES_147_LXXIII-O-08_eng.pdf+&cd=1&hl=en&ct=clnk>.
421 OAS, "Declaration of Principles on Freedom of Expression", Text, (1 August 2009), available at <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26>.
422 "Resolution on Access to Public Information: Strengthening Democracy, AG/RES. 2514 (XXXIX-O/09)" (Organization of American States (OAS), 4 June 2009), available at <http://www.oas.org/dil/AG-RES_2661-XLI-O-11_eng.pdf>.
423 Toby Mendel, (2008) *Freedom of Information: A Comparative Legal Survey*, Second Edition, Paris: UNESCO, p. 144, available at <http://portal.unesco.org/ci/en/ev.php-URL_ID=26159&URL_DO=DO_TOPIC&URL_SECTION=201.html>.
424 Ibid.
425 Ibid.
426 Ibid.
427 Ibid., p. 145.
428 Ibid.
429 Ibid.

disposable for the applicant or extract information from different forms in which it may be held. Many of the systems/techniques used to extract and present such information apply fees regimes. [430] Such fees would relate to the four principal costs involved in the provision of information, namely costs of searching for the information; costs associated with preparing or reviewing the information; costs of reproducing or providing access to the information; and costs of sending the information to requesters. [431]

5.2.4 Limitations and restrictions

The right to information is not an absolute right and will be compromised when conflicting with other equally important rights and public interests. Paragraph 3 of Article 19 of the ICCPR prescribes that the exercise of a right carries with it special duties and responsibilities as restrictions. As observed by the NGO ARTICLE 19, the exception regime is one of the most difficult issues facing those drafting a freedom of information law, since effective laws are undermined in many cases by an excessively broad regime of exceptions.[432] However, it is evidently important that all legitimate secrecy interests are accounted by law in an adequate manner, otherwise public bodies will be required to disclose information that may bring about unwarranted harm.[433]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression examined the limitations on the right, and he recalled that whenever States impose restrictions on the exercise of the right to freedom of expression, these should not jeopardize the right itself. An example could be when the requested information relates to human rights violations. [434] The limitations on freedom of information are legitimate if they meet the narrow conditions defined by the three-part test in Article 19 of the ICCPR, in Paragraph 3.[435]

Although the substantive grounds restricting the FOI right rely on the political, social and cultural circumstances of each country, common elements are found in international and regional FOI laws. Generally speaking, limitations should be set down precisely, clearly and narrowly in FOI law. Article 19 of the ICCPR sets out exclusive legitimate aims in Paragraph 3, namely the respect of the rights or reputations of others; and the protection of national security or of public order, or of public health or morals. A more detailed list of such legitimate grounds, provided by the Council of Europe, includes national security, defence and international relations; public safety; the prevention, investigation and prosecution of criminal activities; privacy and other legitimate private interests; commercial and other economic interests, be they private or public; the equality of parties concerning court proceedings; nature; inspection, control and supervision by public authorities; the economic, monetary and exchange rate policies of the State; and the confidentiality of deliberations within or between public authorities during the internal preparation of a

430 Ibid.
431 Ibid., p. 144.
432 ARTICLE 19, "International Standards: Right to Information", 28 May 2015, available at <http://www.article19.org/resources.php/resource/3024/en/international-standards:-right-to-information#_ftn16>.
433 Ibid.
434 OHCHR, *Report of the Special Rapporteur to the General Assembly on the Right to Access Information*, 4 September 2013, UN Doc. A/HRC/68/362, para. 12, available at <http://daccess-dds-qny.un.org/doc/UNDOC/GEN/N13/464/76/PDF/N1346476.pdf?OpenElement>.
435 OHCHR, Report of the Special Rapporteur to the Human Rights Council on Limitations to the Right to Freedom of Expression, Safety and Protection of Journalists and Media Professionals in Conflict Zones, and Right of Access to Information in Situations of Extreme Poverty, 30 April 30 2009, UN Doc. A/HRC/11/04, para. 11, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/11/4>.

matter.[436] Other specific types of information, whose access is restricted by law, [437] include child pornography,[438] hate speech,[439] defamation, direct and public incitement to commit genocide,[440] and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[441]

436 Recommendation R(2002)2 of the Committee of Ministers to Member States on Access to Official Documents, adopted on 21 February 2002, available at <https://wcd.coe.int/ViewDoc.jsp? Ref=Rec%282002%292&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864>.

437 See UN General Assembly, Report of the Special Rapporteur to the General Assembly on the Right to Freedom Opinion and Expression Exercised through the Internet, 10 August 2011, UN Doc A/66/90, para. 61, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>.

438 Dissemination of child pornography is prohibited under international human rights law. See Office of the United Nations High Commissioner for Human Rights (OHCHR), *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, A/RES/54/263*, 2000, Article 3 Paragraph 1 under C, available at <http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx>.

439 See, for example, HRC, *Robert Faurisson v. France*, Communication No. 550/1993, UN Doc. CCPR/C/58/D/550/1993 (1995).

440 See, for example, Article 38 under c of the Convention on the Prevention and Punishment of the Crime of Genocide. UN General Assembly, *Convention on the Prevention and Punishment of the Crime of Genocide, No. 1021*, 1948, available at <http://webcache.googleusercontent.com/search?q=cache:EQ1HT4W5EHIJ:https://treaties.un.org/doc/Publication/UNTS/Volume%252078/volume-78-I-1021-English.pdf+&cd=5&hl=en&ct=clnk>.

441 See, for example, Article 20 Paragraph 2 ICCPR.

CHAPTER 6 The interplay of privacy, transparency and freedom of expression

6.1 Introduction

The fact that humanity is increasingly embracing the digital age and partly living in new Internet eco-systems is changing the relationships between privacy, transparency and freedom of expression. The previously settled moral norms and laws defining and regulating their conflicts and boundaries, together with the related "rights and obligations", are in the process of being re-delineated. In practice, the conflict and interplay among privacy, transparency and freedom of expression can be analysed at multiple levels and from different aspects in the digital age. This Chapter analyses this interplay from an individual's perspective, discussing how each value may conflict with or complement and support the two other values in the context of daily life realities. While its focus is on the relationship between privacy, freedom of expression and transparency, it also includes a supplementary analysis of the relationship between transparency and freedom of expression.

6.2 Privacy and freedom of expression

The relationship between the right to privacy and the right to freedom of expression is a complex one,[442] which implies that it can be analysed from multiple perspectives and at multiple levels. Both are inalienable human rights and are generally mutually supportive and interdependent. They have a central role along with the values of autonomy, identity and dignity in the realization of human self-development. In the digital age, the two rights are more closely related than ever before in the context of managing and controlling personal information (data) and information flow, insofar as the notion of privacy concerns the concealment of selected personal information. Moreover, the notion of freedom of expression relates to access to, and the disclosure and imparting of, information (including PII at times) in the community.

6.2.1 Interdependence and mutual support

The right to privacy is often considered an essential requirement for the realization of the right to freedom of expression,[443] insofar as privacy protection plays an important role in the creation of the content required for adequate exercising of the rights to freedom of opinion and expression. For instance, it is well understood that individuals need private spaces protected against external pressures and interferences in order to develop their own thoughts, opinions and ideas, which is important not only for self-development but also to promote innovation and social development. It also helps in discovering facts for further communication and dissemination.[444] Privacy protection can also create the context in which individuals can reflect on political change, create counterculture, engage in meaningful critique of society, have creative expressions, and develop their own political

442 Eric Barendt, (2007) *Freedom of Speech*, Second Edition, Oxford: Oxford University Press, footnote 165.

443 OHCHR, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, UN Doc. A/HRC/23/40, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

444 See Rosen's understanding of privacy in the context of knowledge. Jeffrey Rosen, (2001) *The Unwanted Gaze: The Destruction of Privacy in America*, New York: Vintage Books USA.

opinions and artistic expressions, as well as experiment with and formulate views and opinions before making them public.[445]

In short, privacy protection assists with creating the content for unhindered freedom of expression and opinion.

Safe and secured communication is also important to freedom of expression—i.e. including the exchange of opinions and information dissemination—not only from the perspective of the information disseminators but also of the information receivers, as it supports the latter in receiving information free from arbitrary monitoring and interference by others, and in particular by State authorities. More generally, the protection of private spaces against other's interference—be they physical spaces such as home and other private places, or virtual spaces like social network groups— encourages individuals to communicate more freely with each other within a self-defined environment, without fear of unwanted consequences. Respect for privacy of communications is a prerequisite for trust by those engaging in communicative activities, which is successively a pre-condition for the exercise of the right to freedom of expression.[446]

Restrictions on the extent to which offline and online communications may remain anonymous can have an evident chilling effect on victims of all forms of violence and abuse, including by contributing to the fear of double victimization that discourages the reporting of such violence and abuse.[447] In such cases, the protection of privacy is essential to freedom of expression as a notion that encompasses freedom to communicate with other individuals or amongst a selected social group.[448] Thus, privacy protection enhances mutual trust by securing confidentiality among selected individuals, and therefore encourages free flow of information and freedom of expression and opinions among these individuals. The special protection of the confidentiality of journalists' sources is a telling example. In 2013 UNESCO Member States recognized that "privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference".[449] More broadly, in addressing a larger audience or people unknown, anonymity may encourage more free speech and expression about issues of public interest. These points help explain why nowadays encryption and anonymization technologies for anonymous access to, and imparting of, information and communicating securely without being identified, are important for privacy protection and online freedom of expression.[450]

---

445 Daniel J. Solove, (2008) *Understanding Privacy*, Cambridge, MA: Harvard University Press, p. 80.

446 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, p. 95, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

447 OHCHR, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, UN Doc. A/HRC/23/40, para. 24, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

448 Eric Barendt, "Privacy and Freedom of Speech", in Andrew T. Kenyon and Megan Richardson (Eds.), (2006) *New Dimensions in Privacy Law: International and Comparative Perspectives*, Cambridge: Cambridge University Press, pp. 11-12.

449 UNESCO General Conference 37 C/Resolution on "Internet-related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society". http://unesdoc.unesco.org/images/0022/002261/226162e.pdf

450 OHCHR, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, UN Doc. A/HRC/23/40, paras. 13 and 22, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

This is recognized in the Outcome Document[451] of the Connecting the Dots conference endorsed by UNESCO Member States at their 38th General Conference in 2015.

The above is a brief illustration of how privacy protection can strengthen the right or the exercising of the right to freedom of expression. The other side of the coin is that freedom of expression equally strengthens the right to privacy both online and offline, to the point that freedom of expression and its correlative right to freedom of information are critical to the protection of privacy. For instance, freedom of information substantiates disclosures about large-scale data breaches and information privacy invasions—e.g. by big IT companies or by public bodies—which may otherwise not be disclosed. Lack of knowledge and awareness regarding privacy invasions is still a significant obstacle in privacy protection across the world. Edward Snowden's revelations of reported secret mass surveillance led to a global public debate and reforms, which were enabled by free expression on the issue and subsequent FOI requests in various jurisdictions. It has been argued in the Connecting the Dots Outcome Document that: "Illegal surveillance of communications, their interception, as well as the illegal collection of personal data violates the right to privacy and the freedom to hold opinions without interference and can lead to restrictions on freedom of expression".[452]

As interdependent rights, freedom of expression and privacy have an intersection concerning the notion of reputation. On the one hand, defamation law offers protection for the reputation and honour of an individual, which may be linked to the individual's privacy. On the other hand, if defamation law were to offer too much protection for the reputation, honour and privacy of an individual, it could limit others' right to freedom of speech, especially in cases where there is no provision for truth and public interest defence.

Freedom to hold opinions may also be threatened by defamation law when defence of fair comment is not valid. For instance, while the misappropriation of names and likeness—e.g. in identity theft cases—may constitute an invasions of privacy under common law, as well as damage the reputation of some of the individuals involved,[453] freedom of expression also includes satire and caricature, and this may override in certain cases. In other words, there may be either illegitimate or legitimate limitations of either privacy or of freedom of expression, in regards to whether a particular instance of defamatory expression is upheld or not.

The interdependence and mutual support between the right to privacy and the right to freedom of expression are also important for human political life, and especially for improving democracy. Safeguarding the private life and private sphere, will protect political critique and dissent, and allow for political change and development. These underwrite the freedom to vote, hold political discussions and free associations away from the glare of the public and without fear of reprisal.[454] For this reason, adequate protections of privacy, just like freedom of expression, encourage more active participation in politics. The protection of privacy also encourages active political participation by defending the private spheres of political figures and their family members. In the absence of such protection, sensitive people could opt out from public life, distancing themselves and their family members from

451 Outcome Document of the Connecting the Dots conference http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/outcome_document.pdf

452 Ibid.

453 Nathan E. Ray, "Let There Be False Light: Resisting the Growing Trend Against an Important Tort", (1999) *Minnesota Law Review,* Vol. 84, footnote 8.

454 C. Keith Boone, "Privacy and Community", (1983) *Social Theory and Practice*, Vol. 9, No. 1, p. 8.

politics and media scrutiny.[455] How to balance the privacy interests of public figures and persons who participate in public life, with the protection of other's freedom of expression, is always an ongoing dialogue in the practice of law, in all jurisdictions.

Apart from this, the interdependences between the two rights can be witnessed in the context of law enforcement in the Internet age. As UNESCO pointed out in its *Global Survey on Internet Privacy and Freedom of Expression* report, poor protection of privacy has significant impacts on freedom of expression regarding digital communications, across the globe. The Survey reviewed three major reasons in this regard, including the increasing value of open source information to law enforcement due to enabling new technology developments; the difficulty in controlling electronic surveillance as compared to surveillance in the traditional offline world; and the fast growing legal regimes facilitating the use of digital information for law enforcement purposes. The Report also indicates that the combination of poor protection of both privacy and freedom expression led to a multiplier effect,[456] including a chilling effect on online freedom of expression and online privacy interest.[457]

6.2.2 The conflicts and digital intensification

The informational aspect of privacy is about the control and dissemination of personal information within certain self-chosen boundaries by individuals. This may conflict with the fact that the right to freedom of expression protects individuals' freedom to hold, seek, receive and impart information and ideas of all kinds. It also relates to the interest and personal need of data subjects to control information themselves—or through designated parties, and the need of people to access and disseminate information. From a legal perspective, there are in most jurisdictions mutual exceptions or derogations. For instance, Article 10 of the ECHR, in Paragraph 2, prescribes that the exercise of the right to freedom of expression must be subject to "the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary". Then Article 8 of the ECHR, in Paragraph 2, prescribes that: "There shall be no interference by a public authority with the exercise of this right (right to respect for private and family life), except such as is in accordance with the law and is necessary in a democratic society, […] or for the protection of the rights and freedoms of others".

In legal practice, the mutual restriction between the right to privacy and that of freedom expression can be organized in four general types of circumstances, in which an individual's right to privacy conflicts with other individuals' or legal persons' right to freedom of speech.

In the first circumstance, an individual's privacy can be invaded, even if the exercise of freedom of expression and other related rights does not concern the person directly. This

455 The delicate balancing between privacy and freedom of expression regarding public figures, especially, political figures will be discussed separately in Section 7.3. Eric Barendt, "Privacy and Freedom of Speech", in Andrew T. Kenyon and Megan Richardson (Eds.), (2006) *New Dimensions in Privacy Law: International and Comparative Perspectives*, Cambridge: Cambridge University Press, p. 164.

456 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, pp. 95-97, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

457 In the sense that everything you published online can be turned against you in some cases. See Els De Busser, "Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You", (2014) *Groningen Journal of International Law*, Vol. 2, No. 2, available at <http://grojil.org/volume-2/issue-02-privacy-in-international-law/>.

may happen where the mere dissemination of information may lead to the invasion of the solitude or seclusion (and therefore the private sphere) of the individual in an online context. In this context, the special manner in which someone expresses himself/herself and disseminates information, even if merely concerning oneself, may still constitute an invasion of another's privacy, in the sense of breaching the 'leave me alone' meaning of privacy. For example, the Facebook or Twitter account/profile of a user may be flooded with messages and updates from someone, which messages the user would not be interested in at all, but within a context where the user does not have an option to un-subscribe or disconnect for some reason or another. Too much self-expression in social networking sites while ignoring others' expectation for mental solitude and integrity in "a private virtual sphere", may compromise their privacy expectation and infringe the rules of civility that exist in personal relationships.[458]

The second circumstance refers to SPAM (i.e. unsolicited) e-mails, messages, leaflets and similar materials received against the will of the recipient—e.g. in the absence of a subscription by the recipient—even if such communications would be clearly and truthfully framed as of a commercial nature. This is because while such communications would in some senses operationalize the senders' right to freedom of expression, they also constitute intrusions into the recipient's private sphere. In fact, in the offline world, the distribution of door-to-door commercial leaflets is often regulated, allowing the receivers to opt in and/or out by posting stickers on their doors. Similarly, anti-spam laws in many countries—including in the EU and the U.S.—offer opt-in and/or opt-out choices.[459]

The third circumstance refers to the exercise of the right to freedom of assembly, which if not exercised properly can impact on others' right to privacy in both online and offline contexts. While the right to freedom of assembly is protected by many national laws and allowed in manners prescribed by law, even law-permitted assembly may compromise the expectations of private and ordinary daily life that may be held by residents living adjacent to a permitted public assembly venue. Similarly, assemblies and gatherings at private venues or locations without the owner's consent can violate the owner's property right and expectation of seclusion and solitude. The European Court of Human Rights (ECtHR) does not protect the freedom of association across private properties.[460] Online protests or assemblies may take different forms targeting privately-owned Internet spheres, like the widespread DDoS attacks (that are criminalized by Convention 185);[461] organized spamming in comment forums to protest online content; and organized spamming emails against some particular individuals. This raises the issue of how online intermediaries deal with the balance of freedom of association, expression and privacy in their corporate terms of service, and the extent to which private properties entail public space and corresponding entitlements.

The fourth circumstance refers to potential conflicts between an individual, X's, right to privacy and another individual, Y's, freedom of expression when Y's utterances concern X in various ways. This may be when Y tells Y's own story, Y may disclose private information of

458 See the real case of a mother over-expressing her love of the new born on social networking sites of which others have no personal interest to know and complain openly as referred to in Section 2.1 supra.

459 Sylvia Mercado Kierkegaard, "War Against Spam: A Comparative Analysis Of The US And The European Legal Approach", (2015) *Communications of the IIMA,* Vol. 5, No. 2, p. 5.

460 Ian Brown, *Online Freedom of Expression, Assembly, Association and the Media in Europe*, Report, Council of Europe Conference of Ministers Responsible for Media and Information Society, 15 October 2013, p. 17, available at <https://www.coe.int/t/dghl/standardsetting/media/Belgrade2013/Online%20freedom%20of%20expression,%20assembly,%20association_MCM(2013)007_en_Report_IanBrown.pdf >.

461 Ibid., p. 19.

those (i.e. instances of X) who are involved without X's consent, thus potentially breaching X's privacy. For instance, an autobiography author who is a public celebrity in the USA wrote about her sexual life with her ex-husband in detail. Her freedom of speech to talk about her own personal life was in conflict with her ex-husband's interest of privacy.[462] Note that a person has a stronger interest for legal protection in talking about his/her own life, even if this involves disclosures about others, than parties talking merely about other's lives.

In the online world, the invasion of another's privacy in the context of self-expression may also occur through the publication of photographs containing images of not only the individual(s) consenting to the photographs, but also of others, threatening the others' privacy. The occurrence of this type of privacy breach is on rapid increase, due to the proliferation of portable devices and smartphones equipped with high definition cameras, which enable the capturing and generation of information about moments of life, as well as the dissemination of such information to a wide audience of Internet users. Other parties captured in the online disclosed multimedia content may not like being seen by the whole world, thus feeling that such publications compromise their privacy. Extreme cases of this type of privacy breach involve notorious websites on which male users have uploaded intimate pictures of their ex-girlfriends, for revenge.[463] There is also the circumstance of pictures taken solely containing persons other than photographers themselves, whose publication has less protection of freedom of expression right, unless newsworthy or of public interest. This is the reason why German law and French law protect an individual's right to control reproduction of photographs as an aspect of the privacy right.[464] The freedom of expression right may prevail over privacy protection only when there is strong public interest under consideration.

Described above are the common circumstances involving conflicts between privacy and freedom of expression that may occur when the privacy of an individual is compromised by expressions or expressed opinions made by others, or information disclosed by others that do not involve these addressers or speakers themselves, but for personal interest or for achieving certain ends. These types of privacy threats range from the unauthorised disclosure of other's identities, to putting others in false light by publishing untrue, offensive and personal identifiable information to the public, through to publicizing confidential information about them, etc.[465]

In the ECtHR case of *Gurgenidz v. Georgia*,[466] the private applicant, who was a former university teacher, complained that the publication of the information and his photograph in a newspaper by another private person was a violation of the applicant's right to private life as protected under Article 8 ECHR. The defendant argued that the disclosed personal information was published to bring into public attention an issue of suspicious ownership. In the digital age, privacy cases such as this one have been on the rise, concerning rumours, false information and incorrect data regarding individuals flowing freely and thus, threatening individual seclusion and solitude. Numerous cases have been reported across

462 Daniel J. Solove, (2007) *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, New Haven, London: Yale University Press, pp. 135-136.

463 The Editorial Board, "Fighting Back Against Revenge Porn", *The New York Times*, 12 October 2013, available at <http://www.nytimes.com/2013/10/13/opinion/sunday/fighting-back-against-revenge-porn.html>.

464 Eric Barendt, "Privacy and Freedom of Speech", in Andrew T. Kenyon and Megan Richardson (Eds.), (2006) *New Dimensions in Privacy Law: International and Comparative Perspectives*, Cambridge: Cambridge University Press, p. 237.

465 Ibid., pp. 230-240.

466 ECtHR, *En l'affaire Gourguénidzé c. Géorgie*, Judgment, 17 October 2006, Application No. 71678/01 (in French).

the world involving the online disclosure of sensitive private information of victims—mostly adolescents and young adults—for such purposes as online shaming, stalking, harassment, or even monetary gain. These illegal activities have at times even resulted in significant distress, and can potentially trigger suicide. [467]

Many of the privacy-free expression conflicts reported are between individuals and journalists/the media, in that the latter may disclose personal information for a variety of motives, including personal motives, such as to raise public attention for economic benefits, professional reputation, public interest or a mixture of these. Most legal cases against media are brought before court by private litigants—in particular public figures or public celebrities—who regard their privacy as being harmed or under threat. In *Times, Inc. v. Hill*, the USA Supreme Court protected the freedom of expression of the media in the context of the fictionalization of a story by the media that put a family under false light, arguing that: "Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and press".[468]

In Germany, the Constitutional Court ruled in a number of cases, that the inaccurate attribution of remarks violated the privacy of the persons concerned and was not protected by freedom of expression.[469] In such cases, the privacy of ordinary persons is, generally, better protected than that of public figures who willingly or otherwise occupy public roles in social life, unless the disclosed information is newsworthy or of public interest.

Many such conflicts indeed concern public figures or public celebrities and journalists. Public figures and celebrities, unlike ordinary people, occupy a special social status and have social influence over the rest of society, having more channels to react to media disclosures and comments. Journalists and media, on the other hand, often merit special protection for their public function of informing and acting as the watchdog of society. Striking adequate balances between the two significant rights involves delicate work which depends on different cultural-political contexts.[470] In the USA and other jurisdictions, in the pre-Internet era, the public figure doctrine or public figure rule, or similar, has facilitated the striking of balances between the protection of privacy and freedom of expression and provides prediction in law. However, the rise of the digital age, as well as the related power shifts relating to the collection, processing and sharing of information, have altered the two rights' settled scopes, as well as the importance of finding adequate balances between the said rights.

It is worth noting that the right to freedom of information is in some cases not solely granted to individual citizens but also to legal persons. For example, in *Társaság a Szabadságjogokért v. Hungary*, the European Court of Human Rights (ECtHR) decided that a civil society NGO in Hungary had the right to information about the complaint filed by a Member of Parliament. The Court said that the NGO played a role of social watchdog similar to that played by media

467 One of them is Amanda, a Canadian girl abused online by a Dutch adult and killed herself. "Man Charged in Netherlands in Amanda Todd Suicide Case."

468 United States Supreme Court, *Time, Inc. v. Hill* 385 U.S. 374 (1967), 388.

469 Eric Barendt, "Privacy and Freedom of Speech", in Andrew T. Kenyon and Megan Richardson (Eds.), (2006) *New Dimensions in Privacy Law: International and Comparative Perspectives*, Cambridge: Cambridge University Press, p. 240.

470 The balancing of the privacy interest of public figures and freedom of expression will be further analysed below in Section 7.4.

and thus needed such access to publicly-held information of public interest, especially when the request contained no personal data of the MP at stake.[471]

A third circumstance of conflict between privacy and freedom of expression lies in the context of increasingly strengthened State regulation and interference in the digital age. Nowadays, protecting individuals from the escalating large scale data breaches, privacy threats and related harms including online frauds, etc. has been one of the major tasks of national states across the world. State authorities may take advantage of public pressures to seek a kind of privacy protection that restricts the right to freedom of expression of some individuals including journalists and biographers. The protected social group might be government officials or politicians even including the deceased,[472] resulting in restrictions that do not match international standards for legitimate limitations.

6.3 Privacy and transparency

Transparency refers to a cluster of related ideas and concepts such as governmental and organizational action in the open, the availability of information, and accuracy and clarity of the information.[473] According to Schauer, it can be understood in a passive or a negative attribute rather than an activity, like speaking or writing, or a power, referring more to availability and accessibility.[474] A more positive conception of transparency indicates efforts to make information easily usable rather than simply available. Such efforts include, for instance, a requirement of publication as opposed to a requirement of access.[475] As revealed in Chapter 5, transparency can facilitate the realization of good governance and regulation, democracy, efficiency and epistemology in the identification of truth.[476] When reflecting on the roles that transparency has played in the digital age in individual life, the focus of the issue will be on both their conflicts and mutual support that has been enhanced by digital technologies.

Some people argue for personal transparency and urge the acceptance of the idea of "zero privacy" in the digital age, or the notion of "personal transparency". The idea is that transparency is not just an opportunity for institutions to generate trust and be more effective, but also one for individuals to do the same.[477] The more transparent we are to others, the better we will behave morally; and the openness and transparency will render society more tolerant to the bad or embarrassing things that we do, insofar as everyone does so.[478] The risks relating to such openness and transparency can be grouped into risks to one's individual autonomy and dignity relating to the development, management and

471 ECtHR, *Társaság a Szabadágjogokért v. Hungary*, Judgment, 14 April 2009, Application No. 37374/05, paras. 35-38.
472 Bo Zhao, "Legal Cases on Posthumous Reputation and Posthumous Privacy", pp. 90-92.
473 William B.T. Mock, "On the Centrality of Information Law: A Rational Choice Discussion of Information Law and Transparency", (1999) *The John Marshall Journal of Information Technology & Privacy Law,* Vol. 17, No. 4, pp. 1069 and 1078-1081, available at <http://works.bepress.com/william_mock/12>.
474 Frederick Schauer, "Transparency in Three Dimensions", (2011) *University of Illinois Law Review*, No. 4 (2011), pp. 1343-1344, available at <http://www.illinoislawreview.org/article/transparency-in-three-dimensions/>.
475 Ibid., p. 1344.
476 Ibid., pp. 1346-1351.
477 Don Tapscott, "Why Transparency and Privacy Should Go Hand in Hand", *The Huffington Post*, 5 May 2011, available at <http://www.huffingtonpost.com/don-tapscott/why-transparency-and-priv_b_643221.html>.
478 Ibid.

control of personal identity and life;[479] and risks related to the blurring of the difference between individuals and institutions with different social obligations.[480]

From an individual perspective, the conflict between privacy and transparency can lie in the potential threats to privacy from the access to personal information or personal data held by public bodies or other institutions with public functions. In short, the viability and access of personal information to the public should not be in violation of individual privacy. Approached in this way, the conflict of the two values can be viewed as one between the right to information and the right to privacy. The right to freedom of information enshrined by international human rights law grants individuals the right to have access to information "held by public bodies", regardless of the form, source and data of production relating to the information, and in this context 'public bodies' also include other entities when carrying out public functions.[481] The right includes the access to information regarding oneself and to correct such information if not correct, but also includes a right that: "the public and individuals are entitled to have access, to the fullest extent practicable, to information regarding the actions and decision-making processes of their Government, within the framework of each State's domestic legal system".[482]

Information held by public bodies—like information or data of the same nature held by private sector performing public functionalities in the digital age—may, however, concern the privacy of other people who should be protected against potential privacy harm. In this context, accessing and publicly disclosing others' personal data already openly available to the public, in hands of public bodies, may still constitute potential privacy invasion. Such information includes personal information in court records, social programme records, public registers, etc. This category of privacy invasion has been described by the USA Supreme Court as follows: "One did not necessarily forfeit a privacy interest in matters made part of the public record, albeit the privacy interest was diminished and another who obtained the facts from the public record might be privileged to publish it".[483] Further, the Supreme Court added: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information".[484]

In a similar vein with the Court's reasoning regarding computerized information, an increasing threat posed by transparency to individual privacy lies in the collection and profiling of data based upon open-source data and information available to the public, whether online or offline. In one case, two convicted German murderers sued Wikipedia in Germany for disclosing their names on its website after serving their terms. Their request was eventually turned down by the German Federal Court of Justice based on a two-step

479 See also Daniel J. Solove, "Why Privacy Matters Even If You Have 'Nothing to Hide", 15 May 2011, sec. The Chronicle Review, available at <http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/>.

480 Don Tapscott, "Why Transparency and Privacy Should Go Hand in Hand", *The Huffington Post*, 5 May 2011, available at <http://www.huffingtonpost.com/don-tapscott/why-transparency-and-priv_b_643221.html>.

481 "UN Human Rights Committee: General Comment No. 34", 4 July 2011, available at <http://www.opensocietyfoundations.org/publications/un-human-rights-committee-general-comment-no-34>.

482 Human Rights Council, "Resolution Adopted by the Human Rights Council/ Right to the Truth A/HRC/RES/12/12", 12 October 2009, available at <http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G09/165/99/PDF/G0916599.pdf?OpenElement>.

483 "Peck v United Kingdom (2003) 36 EHRR 41", *5RB*, accessed 7 May 2015, available at <http://www.5rb.com/case/peck-v-united-kingdom/>.

484 Ibid., para. 24.

balancing test.[485] However, the Google Spain case was judged on the presumption that easy access to the previous court-ordered bankruptcy finding of the plaintiff (by googling the plaintiff's name) was still a violation of the plaintiff's privacy interest.[486] On other extreme occasions, even parents' access to personal information of their deceased children can be rejected on the ground of a social networking site—e.g. Facebook or Twitter—protecting the deceased's privacy.[487]

But transparency and privacy can also be mutually supportive, improving each other's protection in the digital age. Transparency requirements of data protection law in many jurisdictions require data controllers to disclose sufficient information over the nature of their data processing to data subjects, including instances of data breach, data re-use or change of purpose in use, so that data subjects may know if their personal data and data privacy have been protected according to law. Under the EU's Data Protection Directive 95/46/EC, controllers have the legal duty to provide information to the data subjects in case of processing their data and data subjects have the right to access personal data.[488] The fair processing principle of the EU data protection law requires transparency of data processing, including providing sufficient information to the data subject, including by the notification of data breaches.[489] Transparency in this sense is an important instrument to ensure data privacy protection in data processing.

Another example from the private sector is that in recent years it has become a good practice of some IT giants—e.g. Google, Microsoft, Yahoo, Vodafone, etc.—to publish transparency reports to avert a decline in trust by their customers,[490] hoping also to curtail the appetite of State authority to over-collect data, by opening up the extent of the practice and increasing public awareness. However, there has been lack of transparency on mass surveillance practices from the side of governments, across the world, as regards information engagements with Internet companies and other data controllers. The intermediaries themselves have been slow to disclose records of their own content intervention and identity sharing in response to requests by non-State actors. In a digitized and connected world, in which data processing and data flows are unavoidable, privacy cannot only be protected by means of secrecy and policing regarding what others know about us, like in the pre-Internet age. It can be better protected by stronger transparency and accountability in checking and denouncing questionable behavior concerning the use of collected data.[491]

485 Lawrence Siry and Sandra Schmitz, "A Right to Be Forgotten? - How Recent Developments in Germany May Affect the Internet Publishers in the US", (2012) *European Journal of Law and Technology,* Vol. 3, No. 1, pp. 3-5, available at <http://ejlt.org/article/download/141/222>.

486 Opinion of Advocate General Jääskinen in Case C-131/12 *Google Spain SL Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, delivered on 25 June 2013.

487 Geoffrey A. Fowler, "Life and Death Online: Who Controls a Digital Legacy?", *Wall Street Journal*, 5 January 2013, sec. Tech, available at <http://www.wsj.com/articles/SB10001424127887324677204578188220364231346>.

488 Articles 10, 11 and 12, Directive 95/46/EC.

489 FRA, (2014) *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union, pp. 95-99, available at <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf>.

490 "Google Slams U.S. Government in Latest Transparency Report", *PCWorld*, 14 November 2013, available at <http://www.pcworld.com/article/2063386/google-slams-u-s-government-in-latest-transparency-report.html>.

491 David Brin, "Why Transparency will save Privacy", Text, *The European*, 16 October 2013, available at <http://www.theeuropean-magazine.com/david-brin--2/7535-why-transparency-will-save-privacy>.

The other side of the coin is that good privacy protection can help with achieving more transparency in other areas of information. This link is based on institutional actions for both government and private companies in improving trust that transparency will not violate the privacy of personal information. Strong privacy protection of personal information and data privacy such as via Privacy Enhancing Technologies (PETs) will be a big advantage for companies in market competition and will encourage customers to give their personal information for service. There is also no doubt that good protection of information privacy and personal data by State authorities will improve government-citizen interaction in data processing, which in turn promotes transparency with more trust in government and more willingness to offer personal data by individual citizens. According to a recent report, transparency "requires public confidence, and one way to ensure that is to reassure the public that its privacy is a central concern whose protection is embedded in decision-making processes".[492]

6.4 Transparency and freedom of expression

Transparency itself is not a fundamental value equal to privacy and freedom of expression, but one derived partly from the right to information and partly for its value in enhancing democracy and other public goods including mutual trust, societal corporation, efficiency, justice, equality, anti-corruption, accountability and good governance. Transparency as a political end can be achieved by protecting and granting access to, and proactive disclosure of, desired information by the general public, for instance, by legal instruments protecting the right of freedom of information. When this right is well protected, the value of transparency is secured as a public good or a public interest. Transparency can also be strengthened by an environment in which press freedom and the right to impart information and opinion are well protected. In this sense, Schauer has pointed out that free speech may be best understood as a component, even if not the most important component, of a larger commitment to transparency.[493]

From the perspective of information control and management, transparency and freedom of information approach information flow from different endpoints. Transparency concerns the accessibility of desired information from the side of information or data controllers, and relates to the availability and usability of such information when requested. Freedom of expression and freedom of information refers to individuals as the subjects disseminating and accessing information for desired purposes. Freedom of expression and freedom of information are positive entitlements, while transparency is rather the desired open state in information flow.

For individuals, transparency and freedom of expression and opinion are mutually supportive and supplementary to each other. Without transparency, in particular in terms of transparency as epistemology,[494] freedom of expression makes less sense in imparting, receiving and accessing information when such information is broadly closed and not open to scrutiny in terms of truth and facts. It is recognized that transparency of ownership

492 Kieron O'Hara, "Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office", 27 March 2014, p. 3, available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61279/transparency-and-privacy-review-annex-a.pdf>.

493 Frederick Schauer, "Transparency in Three Dimensions", (2011) *University of Illinois Law Review*, No. 4, p. 1356, available at <http://www.illinoislawreview.org/article/transparency-in-three-dimensions/>.

494 That the open availability of information will facilitate the identification of truth and falsity and consequently produce more knowledge and greater progress. See Ibid., p. 1350.

is the precondition of independent media.[495] In addition, transparency can and must be facilitated by freedom of expression and freedom to information, in that the availability and accessibility of information held by public bodies and other institutions with public duties per se does not mean that such information will reach the hands of those who need it. There is always a gap in the information flow chain between individuals and government bodies, which needs to be bridged by the exercise of press freedom and the wider freedom of expression by individuals, such as providing requested information and the related source online. Through the protection of online freedom of expression, transparency and in particular institutional transparency will be largely improved.

6.5 Balancing privacy, freedom of expression, the right to information and transparency: practices and critiques

As important human values and public goods, the optimization of these ends is the highest goal of human community because of the conflicting interests among individual citizens and diversified social groups. Balancing these values involves considering many variables important to society, and the criteria that any limitation of rights should be: a) prescribed in law; b) necessary; c) proportionate; and d) for legitimate purpose.[496] Generally speaking, there are two categories of balancing: balancing by definition and *ad hoc* balancing. [497] These are especially relevant to the cases of freedom of expression and privacy, and can also apply to the right to information and transparency.

Balancing by definition

The first approach is to define the precise scopes of each right by setting out clear rules to prevent potential conflict; for instance, by explicitly prescribing what genres of speeches are not allowed because they violate another's privacy without meeting the international standards such as the test of necessity. Examples may be the confidentiality duty of those working at post office, law firms and medical services not to disclose their customers' information to third parties. Limitations of confidentiality in such cases would have to be shown as necessary; for example, for law enforcement in the sense of being the only way to secure another right such as the right to security of the person. In data protection laws, data controllers usually have the legal duty not to transfer controlled personal data to a third party without the consent of data subjects.

Recital 39 of the European Data Protection Directive 95/46/EC (DPD) prescribes that: "whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party". [498] Article 9 of the DPD sets out categorical exemptions: "Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression

495 Access Info Europe, "Special Rapporteurs on Freedom of Expression Called to Endorse Transparency of Media Ownership", available at <http://www.access-info.org/tmo/15958>, accessed 8 September 2015.

496 When balancing concerns rights online, UNESCO advocates that the exercise also take account of the principles of Openness, Accessibility and Multi-stakeholder participation (see below)

497 For a distinction of the two concepts of balancing, see T. Alexander Aleinikoff, "Constitutional Law in the Age of Balancing", (1987) *The Yale Law Journal,* Vol. 96, No. 5, p. 948.

498 Directive 95/46/EC, recital 39.

only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression".[499]

The limitation of freedom of expression in the interest of privacy would also need to be justified by the necessity criterion, and hence the proportionality principle. However, both rights can be limited by other imperatives. The law-prescribed derogations or limitations include extreme circumstances with international consensus such as the dissemination of child pornography materials. It is a universal practice of national laws, as revealed by the UN Human Rights Council, to forbid harmful speeches including online child pornography which violates children's dignity and privacy.[500] Other materials that are variously restricted are hate speeches which amount to advocacy of incitement to violence, hostility or discrimination, including those related to gender, race, sexual orientation and religion.[501] In some European countries such as France and Germany, Holocaust denial speeches are forbidden by law too. The privacy of those persons expressing such views may be limited in order to establish the identity of the actors involved for the purposes of law enforcement. Balancing rights in the case of adult pornography may depend on the interpretations of public morality, and neither expression nor privacy may be protected accordingly.

A significant benefit for the balancing by definition is that this should normally occur through legislation that can open the issue for sufficient public discussion and debate, before taking a decision on the potential scope, procedure, elaboration of derogations, and public interest exemptions. In the case of private intermediaries performing balancing by definition, this should be outlined in terms of service.

Ad hoc balancing

Much actual balancing practice has been done by capable courts—i.e. supreme courts, constitutional courts, regional courts or national courts—in an *ad hoc* manner. In this context, conflicts are resolved by deliberating on new circumstances, before adjudicating courts, with the intention to re-define or re-delineate the legal boundaries for privacy and free expression by gradually developing case law in that area. Though there are differences in the balancing mechanisms used in the various jurisdictions, and in the gravity that they grant to the two rights, such balancing mechanisms or processes usually follow the test that is well addressed by the Human Right Committee's General Comment 27.

Accordingly, to assess whether a limit can be justified, the limit should satisfy criteria such as: a) any restrictions must be provided by the law; b) the essence of a human right is not subject to restrictions; c) restrictions must be necessary in a democratic society; d) any discretion exercised when implementing the restrictions must not be unfettered; e) for permissible restriction, it is not enough that it serves one of the enumerated legitimate aims, but it must be necessary for reaching the legitimate aim; and f) restrictive measures must conform to the principle of proportionality, meaning that they must be appropriate to

499 Ibid., Article 9.

500 UN General Assembly, Report of the Special Rapporteur to the General Assembly on the Right to Freedom Opinion and Expression Exercised through the Internet, 10 August 2011, UN Doc A/66/90, para. 21, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290>.

501 See in general UNESCO, "Countering Online Hate Speech", June 2015, available at <http://www.unesco.org/new/en/media-services/single-view/news/unesco_launches_countering_online_hate_speech_publication/#.Ve8wA5e5wg4>.

achieve their protective function; be the least intrusive instrument among possible means for the same result; and be proportionate to the protected interest.[502]

As UNESCO pointed out in the report presenting the results from the global survey on Internet privacy and freedom of expression, a public interest test is also a popular criterion applied in balancing the two rights, in deciding which right shall prevail. This has been well established in two ECtHR's *Von Hannover v. Germany* cases,[503] which concern: a) the conflict between the right to freedom of expression (in particular regarding mass media) and the privacy right of public figures; and b) the conflict between the right to privacy of individuals and the right to access information held by public bodies.[504]

The balancing practice of the European Court of Human Rights includes the case of *Axel Springer AG v. Germany*,[505] in which the Court set forth a number of conditions for achieving good balancing of the media's right to freedom of expression and the public figures' right to privacy. These conditions include: a) contribution to a debate of general interests; b) how well known are the person concerned and the subjects of the report; c) prior conduct of the persons concerned; d) the method of obtaining the information and its accuracy; e) the content, form and consequence of the publication; and f) the severity of the sanction imposed.

In *Hachette Filipacchi Associés v. France*, the privacy interest of the family of a dead local French politician was at stake due to the publication of some death-scene photos. The Court investigated the legality of the State authority's interference with the complainant's freedom of expression, testing whether the State interference fulfilled the requirements of "prescribed by law", "legitimate aim", "necessary in a democratic society", and proportionality or severity of the interference. [506] In *Peck v. the United Kingdom*, the Court ruled that the disclosure of two photographs taken from the CCTV footage covering the unmarked images of the plaintiff, as a private person, was disproportionate and constituted unjustified interference with the plaintiff's private life, and violated his right as protected by Article 8 of the ECHR.[507] Balancing as a way to optimize human rights, as in the case law of ECtHR, has been implemented by European jurisdictions such as in the German law and other EU Member States.

However, the balancing of fundamental rights in general is not immune to critiques. Some argue that accepting the assignment of different weights to some human rights, where such weights depend on the circumstances framing a particular case, gives a shifting character to human rights principles. They also argue that the process of balancing can possibly swallow up the rights. One solution against such critiques is to stick to the proportionality principle, by limiting power for interference.[508]

---

502 Ct OHCHR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, *Frank La Rue*, 17 April 2013, UN Doc. A/HRC/23/40, para. 29, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

503 Toby Mendel et al., (2012) *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Series on Internet Freedom, Paris: UNESCO, pp. 98-99, available at <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-Internet-privacy-and-freedom-of-expression/>.

504 Ibid.

505 ECtHR, *Axel Springer Ag v. Germany*, Judgment, 7 February 2012, Application No. 39954/08.

506 ECtHR, *Hachette Filipacchi Associes v. France,* Judgment, 14 June 2007, Application No. 71111/01, paras. 29-65.

507 ECtHR, *Peck v. United Kingdom*, Judgment, 28 January 2003, Application No. 44647/98.

508 Başak Çalı, "Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions", (2007) *Human Rights Quarterly*, Vol. 29, No. 1, pp. 253-254.

Another important issue is the assumption that each balanced right involved in a balancing process is commensurable, which treats such rights as constructs that are context-sensitive, subject to utilitarian calculations of net benefit, which would run against the nature of human-right protection itself.[509] Last, the public interest test exercise that is popularly applied in the practice of balancing the two rights can be problematic, insofar as it may create an artificial conflict between the individual and the collective. The nature of human rights should not be about the interest of a particular person, but about those of each and every person. [510]

For its part, UNESCO, as part of the UN system, directly follows the principles set out in human rights documents for the reconciling of rights, namely the need for legality (and therefore predictability), necessity (and thence proportionality), as well as legitimate purpose. In addition, the objective of ensuring the least invasive solution is acknowledged, so that the essence of each right should not be impaired, and that limitations should be exceptional in nature. In regard specifically to hate speech, which entails balancing the expression of some with rights of others to dignity, equality and security (amongst others), UNESCO takes cognisance of the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[511] This document of the UN Office of the High Commissioner on Human Rights goes beyond the "three part test" noted above, and outlines an additional six-part test. In terms of the latter, imposing restrictions on hateful speech should be decided only after assessing the context, the status and intent of the speaker, content and reach of the expression, and the likelihood including imminence of harm. To supplement all this, when it is a question of reconciling rights specifically on the Internet in particular, additional considerations may come into play. Such considerations are evident in the concept of Internet Universality adopted by UNESCO's Member States in 2015. The concept calls for Internet decision-making to take cognisance of Human Rights, Openness, Accessibility and Multi-stakeholder participation (the 'ROAM principles'). Accordingly, to preserve the universality of the Internet, the balancing of rights online should also consider any potential impact on the Openness and Accessibility dimensions of the Internet, and be achieved via multi-stakeholder processes.[512]

509 Ibid., p. 259.
510 Ibid.
511 http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf
512 See http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/sakharov_seminar

CHAPTER 7 What is missing: a gap analysis of the status quo

7.1 Introduction

The proliferation of the Internet and increasing uses of novel mobile computing devices have raised numerous practical risks for, and challenges to, the rights of privacy, freedom of expression and freedom of information. Some of the threats underpinning such risks and challenges—at the individual, national and international levels—have already been illustrated in Chapter 2. So this Chapter elaborates further, by exploring the major threats to personal privacy and freedom of expression that emerge from advanced digital technologies. Section 7.2 contains a discussion of issues linked to privacy protection technologies and designs based on a detailed analysis of the privacy threats that emerge from recent related technological advancements, and it illustrates flaws in existing legal protection mechanisms. Section 7.3 provides an introduction regarding emerging threats to freedom of expression in online contexts. Finally, in section 7.4, which concludes the chapter, the focus is shifted to techniques that may be used to balance the two human rights in the digital age, as well as to three concrete cases that relate to such techniques.

7.2 Online privacy and data protection

7.2.1 New technologies and new privacy threats

Though the traditional laws and social norms have been adapting to the rapid evolutions in Internet eco-systems, including to increasingly blurred boundaries in human interaction, rapid advances in ICT have persistently been steps ahead of reforms. If it is fair to assume that Moore's Law will continue to apply during the next decade, such that we continue to experience rapid increases in computer processing power and storage capacities, as expected, then it is also reasonable to predict that significant advances in all aspects of ICT and the online environment will continue to influence individual privacy in many ways, and potentially more than ever before. This is likely to contribute to additional gaps and deserves due attention from policy and law makers.[513]

One such influence on individual privacy is expected to result from the emergence and growth of the 'Internet of People' (IoP) and the 'Internet of Things' (IoT), especially when combined with continued advances in nanotechnology. The IoP and the IoT are anticipated to significantly extend the Internet from what it is to a network or group of networks that connect a substantially wider range of objects or groups of objects—e.g. including objects like home appliances (such as fridges and cookers); transportation vehicles (such as cars and trains); RFID-tagged items (such as living animals and stored items); and groups of nanosensors (such as ones injected into living bodies or into environments)—which will be assigned unique identifiers; e.g. IP addresses. The IoP and IOT, in doing so, are expected to constitute PITs, in that they shall enable the exercising of more control over data that fits current and/or future definitions of 'PII', including the collection, storage, processing and transmission of data—such as geo-location information, user-activity patterns, communication data, etc.—that will ultimately facilitate the creation of data profiles

513 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 3, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

regarding those who use IoP- and/or IoT-connected devices and those regarding whom PII is captured by IoP- and/or IoT-connected devices.

Thus, it is clear that the combination of the IoP, the IoT and nanotechnology has the potential of generating vast amounts of data that either constitute or could be analysed to extract PII or other data that may lead to privacy breaches. More specifically, such combination of technologies and the resulting data can enable such activities as the generation of smart data, data profiling regarding people, and the seeking of underlying hidden patterns and unexpected correlations that lead to privacy breaches. For instance, future nanotechnology may enable the widespread automatic analysis of data collected from nanosensors implanted into one or more human bodies to determine facts about individuals' health. Similarly, the scanning—and therefore the powering and reading—of a passive RFID implanted in a pet can generate data that alone or combined with other data would enable burglars to deduce or make educated guesses regarding whether the pet's owners are likely to be at home. Similarly, data profiling can enable the identification of individuals by means of analyses of the individual's behavioural patterns, allowing leeway under present legal protection frameworks.[514]

Additionally, note that such predictions do not account for the possibility that individuals or institutions could themselves become able to produce passive or active nanosensors and devices. If such ability would exist, then it could greatly enhance the range of attacks that could be devised against people and their assets. For example, it could be convenient for an individual to illegally and unethically use nanosensors to determine facts about the medical condition of someone to subsequently blackmail that person by threatening the publication of his or her medical condition, thus impinging on a wide range of rights. Moreover, since the combination of the IoP, the IoT and nanotechnology could facilitate the generation of vast amounts of data that may themselves constitute, or lead to the extraction of PII or other privacy-breaching data, such combination may also increase the risk of the occurrence of privacy breaches by the illegal and/or unethical access by third parties of the data collected and/or analysed.

Another critical risk and challenge to individual privacy emerges from the promising practice of Cloud computing, which conceptually refers to the reorganisation of how computing infrastructure (e.g. processing power and disk storage space), platforms (e.g. SNS platforms like Facebook and Twitter) and software (e.g. webmail systems like Google mail) are made available, publicly and/or privately, for use by the general public, corporates and other types of users. Using more mainstream terminology, these types of reorganisation are generally referred to by the following terms, respectively: a) 'Infrastructure as a Service' (IaaS); b) 'Platform as a Service' (PaaS); and c) 'Software as a Service' (SaaS); as well as collectively by the term 'Everything as a Service' (EaaS).[515]

Despite the related benefits, Cloud computing raises significant data safety and information privacy concerns. Firstly, individuals' data stored on Cloud-based storage locations (e.g. Dropbox, OneDrive or Google Drive) will be stored at a range of unknown places, thus

514 See the discussion of the problems of PII in the U.S. law context by Schwartz and Solove. Paul M. Schwartz and Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", (2011) *New York University Law Review*, Vol. 86, pp. 1836-1864, available at <http://papers.ssrn.com/abstract=1909366>.

515 "The Future of Cloud Computing - Opportunities for European Cloud Computing beyond 2010", p. 1, available at <http://ec.europa.eu/digital-agenda/en/news/future-cloud-computing-opportunities-european-cloud-computing-beyond-2010>, accessed 14 May 2015

being subject to different jurisdictions that provide different, and possibly inadequate types of privacy protection. For instance, current data protection legislation in Europe does not provide adequate solutions to the challenging problems uniquely linked to all aspects of the Cloud,[516] negatively influencing both transparency in the Cloud and the exercise of freedom of expression broadly, including press freedom and the right to information. Secondly, Cloud computing—especially combined with such other technologies as distributed computing and grid computing, and with the availability of vast amounts of data—can facilitate information security breaches and privacy breaches. An example is that, insofar as vast amounts of processing power—as may be offered by the combination of millions of computer processors—could facilitate exhaustive searches which enable the illegal and/or unethical decryption of 'ciphertext' (encrypted plain text), or the de-anonymisation of data that would otherwise remain anonymised.

Other risks and threats to privacy emerge from the spread of biometric technologies, of which the main function is to authenticate relevant individuals' live-ness and identity and which is based on the measurement and recording of their unique and distinctive physical, biological and behavioural characteristics, including their fingerprints, facial features, iris, voice, hand geometry, vein patterns, gait and DNA. Recently, biometric technology may also involve the use of genome data and 'proteomics' (the large-scale study of proteins), which can enable the identification of markers for specific diseases and treatments,[517] and which can also uniquely identify individuals. The use of these technologies has been increasing in the past decades in many contexts, including: a) public administration tasks, such as the registration of the identity of individuals in border control environments; and b) the administration and management of access to, and the enjoyment of rights. Such rights may cover civil rights, like the right to vote, and social rights, like the rights to health care and education.[518]

From a rights' perspective, the use of biometric technologies poses serious risks and threats to privacy both intrinsically, insofar as it may lead to the unique identification of individuals, as well as to the breach of PII about the individuals being authenticated; and indirectly, because it may have a bearing on freedom of expression issues broadly, such as by discouraging privacy-aware citizens from engaging in the exercising of their right to freedom of expression, including right to information. Other related risks, which may materialise subsequent to and/or in the breach of these rights, include: a) fraud, theft and misuse (e.g. weaknesses in a biometric system leading to information leaks that may facilitate the illegal altering of financial records); b) misidentification and inaccuracies (e.g. false positive authentications leading to inappropriate access to PII); c) being exclusionary (e.g. biometric systems not equally functional in authenticating individuals from different ethnic backgrounds, or individuals with different capabilities); and d) the misuse of biometric

516 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, pp. 8-9, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

517 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 7, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

518 Privacy International, "Biometrics: Friend or Foe of Privacy? | Privacy International", p. 4, available at <https://www.privacyinternational.org/?q=node/48>, accessed 14 May 2015.

data (e.g. to facilitate passive surveillance or data retention that breach the rights of the individuals involved).[519]

Big data and big data analytics—which in short refer to the accumulation and exploitation of vast and complex information databases,[520] where the data contained in such databases includes data produced by and about people, things and/or the interactions between them[521]—are capable of results that may have significant impacts on individual privacy. The use of big data technologies, particularly in the absence of transparency, raises several privacy concerns, including regarding: a) the anonymity and pseudonymity of the data subjects; b) the re-use of data with changed purposes; c) the data subjects' consent; d) lack of information regarding the accuracy of personal data; e) profiling by unknown data controllers; and f) the sacrifice of information privacy in the absence of relevant information security checks and balances. The use of big data technologies also raises other issues, including in relation to: a) discriminations about the data subjects; and b) mistaken pattern-matching.[522]

One of the most significant risks to individual privacy relates to the mass- and targeted-surveillance activities that may occur in combination with some or all of the aforementioned technologies and/or other technologies.[523] Today's mass-surveillance activities include the use of well-known technologies and techniques, such as: data profiling, based on shared databases and collected data; the processing of communications data and meta data; geolocation tracking through multiple portable devices; Deep Package Inspection (DPI); malware, such as tracking malware and pre-installed backdoors; hacking tools and techniques, such as social engineering, pharming and phishing; social media monitoring; automated and manual Internet activity monitoring;[524] and the use of CCTV systems and other data collection mechanisms. Such widely-acknowledged surveillance activities are accompanied by others that are either unknown or less known to the general public, such as the once less-known voice-processing technologies.[525]

7.2.2 Problems of privacy protection technologies and designs

Many scholars and policy makers promote Privacy by Design (PbD) as a default solution for the protection of individual privacy and freedom of expression online, and consider the use of Privacy Enhancing Technologies (PETs) to achieve better levels of online privacy; e.g. ones that enable: i) the anonymisation and pseudo-anonymisation of data; ii) the use of

519 Privacy International, "Biometrics: Friend or Foe of Privacy?", pp. 10-15, available at <https://www.privacyinternational.org/?q=node/48>, accessed 14 May 2015.

520 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 5, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

521 Primavera De Filippi, "Big Data, Big Responsibilities", (2014) *Internet Policy Review: Journal on Internet Regulation*, Vol. 3, No. 1, p. 1, available at <http://policyreview.info/articles/analysis/big-data-big-responsibilities>.

522 Ibid., pp. 2-7.

523 For an explanation of the two categories of surveillance, see OHCHR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, *Frank La Rue*, 17 April 2013, UN Doc. A/HRC/23/40, paras. 33-40, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

524 See a short summary of the employed technologies, see Ibid., paras. 7-13.

525 Dan Froomkin, "How the NSA Converts Spoken Words Into Searchable Text", *The Intercept*, available at <https://firstlook.org/theintercept/2015/05/05/nsa-speech-recognition-snowden-searchable-text/>, accessed 15 May 2015.

cryptosystems and cryptographic primitives to achieve data confidentiality; and iii) the use of network security components, such as firewalls and onion-routing techniques to protect communications.[526] However, PbD and PETs are not absolute, and they often themselves present privacy-related and other issues.

As Korff and Brown stated in 2013[527], the key to suitable anonymisation does not revolve around the removal/replacement of direct identifiers from the relevant data—even when these removals/replacements would be complemented by the encryption of the underlying data—but around the size of the 'anonymity sets'—i.e. 'data pools'—that contain the anonymised data. Indeed, anonymization techniques involving the mere replacement of direct identifiers will be compromised when more and bigger data/anonymity sets are available for such activities as big data analytics, insofar as more data increases the possibility of discovering the identities linked to the anonymised data. Suitable solutions to such problem would include: a) transparency—i.e. lack of reliance on 'security by obscurity'—regarding the anonymization technologies adopted, enabling open peer-reviewing that will ultimately enhance security; and b) adequate procedures for disclosure, enabling early warnings to all the relevant parties. This said, like in many other security contexts, the key objective in the use of anonymization technologies is not to achieve absolute anonymization; rather, it is to ensure that the costs involved in achieving de-anonymization outweigh the benefits—i.e. from the intruder's perspective—that may emerge from such de-anonymization.

PbD is widely recognized as lying ahead of PETs in the protection of privacy in online and other contexts, largely because it involves the adoption of built-in safeguards at the design stage of the development of services and/or artefacts (i.e. in ex-ante), rather than the bolting of safeguards onto existing services, technologies and/or artefacts as an afterthought, or late in the development lifecycle (i.e. in ex-post). The circumvention of PbD is essentially meant to be practically impossible or exceptionally difficult, because it requires forcing of the system or device to perform an act that it is not designed for.[528] PbD solutions also go beyond PETs insofar as they may lead to measures that go beyond what is generally achieved as an afterthought; e.g. not only at the technological (i.e. hardware or software) level but also the physical, procedural, legal and other levels. Other characteristics of PbD-based solutions include that these: a) are often unique and tailored to the service or artefact being designed; b) are technology or device concerned; and c) are developed to address any specific threat to privacy.[529]

However, PbD has its own challenges and limitations. A significant issue lies in the satisfaction or manifestation of existing legal norms, prescriptions and principles in the design of online solutions and the underpinning technologies. For instance, it is often difficult to bridge the gap between legal language (which is relatively ambiguous and imprecise) and the

526 Onion routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. See Michael G. Reed, Paul F. Syverson and David M. Goldschlag, "Anonymous Connections and Onion Routing" (1998) *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 4, p. 482.

527 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, pp. 17-18, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

528 Demetrius Klitou, (2014) *Privacy-Invading Technologies and Privacy by Design*, Vol. 25, Information Technology and Law Series, The Hague: T.M.C. Asser Press, p. 271, available at <http://link.springer.com/10.1007/978-94-6265-026-8>.

529 Ibid., pp. 270-272.

precision normally involved in the design, development, testing and implementation of computerised systems. It is also difficult to balance the benefits and costs that emerge from both specificity and flexibility. And there are definitional problems too, such as regarding what constitutes personal data under PbD.[530] Additionally, the European Union Agency for Network and Information Security (ENISA), having analysed the limits of PbD from a technical perspective, has called for further research on the challenges relating to PbD, its application and the underpinning methods and techniques, which range from: a) the fragility of privacy properties; to b) privacy metrics and utility limitations; to c) increased complexity; and to d) obstacles to the implementation of PbD, such as unclear or too narrow interpretations relating to the function of PbD.[531]

In general, the use of technology to achieve anonymity in communications—e.g. single proxies, Virtual Private Networks (VPNs), onion routing, mesh-networks, and encryption technologies by most service providers—will go a long way in averting privacy invasion activities. However, some individuals' use of such technologies will, paradoxically, often attract interception and monitoring by State authority, especially since most online users still employ poor privacy protection mechanisms. Furthermore, the use of technology to achieve anonymity/privacy online can hinder law enforcement activities, including in relation to the fight against online-enabled crimes relating to the rights discussed in this Report. For instance, it will be more difficult to identify who violates freedom of expression—e.g. in defamation and hate speech—if the perpetrator employs anonymization technology to hide his/her identity.

7.2.3 Defective legal protections

As previously indicated, the evolution of the laws and regulations for the protection of privacy in online contexts has been slow compared to the corresponding advances in technology. Given that it is not possible to cover all the legal and policy gaps relating to the protection of privacy in this Report, this section is limited to a thematic illustration that outlines the major problems. The lack of regulatory action is becoming rather serious and particularly in view of the following thematic circumstances.

The first problem relates to the conceptual definitions adopted in different jurisdictions and legislations. As Bygrave noted in 2015, ICT law is increasingly characterized by the mixture of law and technology terms that may not fit well into each other, leaving gaps and conflicts in the implementation of law.[532] For instance, with fast advances in ICT, the commonly used legal concept of PII is insufficient and subject to updates.[533] Similarly, different laws and jurisdictions around the globe adopt different definitions for the same term—e.g. for the term 'personal information' as used in data protection and Freedom of Information (FOI) law—achieving different levels of clarity and contents.[534] Definitional conflicts relating to

530 Ibid., pp. 284-286.

531 ENISA, *Privacy and Data Protection by Design: From Policy to Engineering*, Report, December 2014, pp. 48-49, available at <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design>, accessed 24 April 2015.

532 Lee A. Bygrave, "Information Concepts in Law: Generic Dreams and Definitional Daylight", (2015) *Oxford Journal of Legal Studies*, Vol. 35, No. 1, pp. 91-120.

533 Paul M. Schwartz and Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", (2011) *New York University Law Review*, Vol. 86, available at <http://papers.ssrn.com/abstract=1909366>.

534 David Banisar, "The Right to Information and Privacy: Balancing Rights and Managing Conflicts", World Bank Institute Governance Working Paper, 10 March 2011, p. 19, available at <http://papers.ssrn.com/abstract=1786473>.

such terms may also exist within the same jurisdiction; e.g. in the case of how the Irish define 'personal information' in their Data Protection Act (DPA) and FOI law.[535]

It is useful to note that such problems are on the rise with advances in ICTs, partly because new technology—e.g. that triggering the growth of categories of biometric data, and their use—continues to shape society's understanding of such concepts as 'PII'. And partly because novel technology will raise the need for novel terms and/or definitions for existing terms that are recognised as broad and/or vague, such as: 'law enforcement', 'serious threats', 'national security', 'morals' and 'public order'. An additional problem relating to such definitional deficiencies is that these are, paradoxically, derogating the privacy protection of individuals. Indeed, such shortcomings threaten even the scope of the right to privacy enshrined by international human rights law; e.g. by means of vagueness in the right's application.[536] Thus, it is clear that more specific and concrete conceptual approaches must be adopted to secure the right to privacy and data protection.

The second problem relates to lack of legislation/regulation regarding the phenomenon of 'data profiling'. As seen most recently from various privacy reports, this activity has become a major concern to privacy advocates, with the most worrying aspect being the data connectivity and/or linkability that is facilitated by the sharing of all sorts of databases amongst different data controllers. This often results in data subjects being unaware of, and lacking the means to discover what is happening in the 'black box', especially when the data being processed is categorized as anonymous or pseudonymous. Another issue relating to such data profiling is that it involves collaborations between the business sector and public authorities, where the former has defined business models that render it—and the underpinning data collection, storage and processing—profitable; and the latter find it useful, especially for the purposes of law enforcement and intelligence. Data profiling, framed within such a context, is especially problematic because, as noted by Korff and Brown, decisions made by either public authority or private sector on individuals for different treatments can be unfair and discriminating; and where grounds are unknown to individuals, the experience of injustice finds no proper remedy.[537]

The third privacy-protection problem relates to lack of legislation—at both the national and international levels—regarding the cross-border transfer, storage and/or processing of data, which is on the rise globally, especially due to the increasing tendency towards the outsourcing of the processing and storage of data to the private sector; e.g. by means of Cloud computing. The main concern is about the processing of large quantities of data in foreign territories, under the laws of one or more foreign jurisdiction(s). The nature of such data varies significantly, ranging from: passenger name records (PNRs) to shared data used in mutual legal assistance and agreements against crimes, to online commercial transactions, to online gaming, to SNS-based interactions between users, etc.

The EU has made considerable efforts to secure data safety in cross-border data transfers, by establishing legal requirements for data controllers in Data Protection Directive 95/46/EC, and by means of the Safe Harbour Program, however such efforts have not led to the

535 Ibid.

536 OHCHR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, *Frank La Rue*, 17 April 2013, UN Doc. A/HRC/23/40, para. 21, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

537 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 30, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

desired results. At the time of writing, the Safe Harbour had been overtaken by the 'Privacy Shield', but the latter was also not without controversy in terms of protecting Europeans' rights. For national States, the protection of the safety and privacy of their citizens' data abroad is a legal obligation to fulfil by means of proper legal and diplomatic measures. It seems that for many States personal data protection is not taken as an independent human right *per se*. In terms of the present international law framework, in many cases no effective legal remedies exist, for both minor or major data and data privacy breaches.[538] Through what has been called 'data nationalisation', some States have relocated data storage and processing in attempts to reduce cross-border transfers, achieving dubious results that may lead to undesired effects, e.g. the fragmentation of the Internet. In general, the privacy problem of the cross-border transfer, storage and processing of data is subject to further international agreement and cooperation.

The fourth privacy-protection problem relates to lack of updates in many countries' legal frameworks, which contribute to not addressing the threats and challenges that emerge from widespread communications surveillance in the digital age.[539] The State authorities' increasing electronic interception capabilities—which often occur for law enforcement purposes, intelligence service purposes, or for both purposes at the same time—can compromise the privacy interest of individuals, partly due to insufficient procedural protection relating to the processing of the personal information and data for such purposes, which is collected by public bodies themselves, or acquired from the private sector. In particular, the exterritorial mass surveillance activities carried out by some States in foreign territories are controversial because of their significance to the data subjects' right to privacy and equal protection. This is why the UN General Assembly has called for reviews, and why many actors, including Internet intermediaries, call for the recognition of mechanisms, such as the Mutual Legal Assistance Treaties (MLATs), and for respect for the European Convention on Human Rights and Convention 108.[540]

7.3 Freedom of expression online and further improvements

According to a 2014 Freedom House report, Internet freedom is declining in 36 out of the 65 countries assessed. The key reasons provided are: a) the proliferation of repressive laws; b) new regulatory controls over online media; c) increased surveillance; d) increasing arrests of SNS users; e) intensified demands on the private sector to disclose information; f) new threats facing women and the lesbian, gay, bisexual, transgender and intersex (LGBTI) population; and g) more sophisticated and widespread cyber-attacks.[541] In line with this, according to UNESCO's recent Internet survey, arbitrary blocking, filtering and content regulation are still a major factor that hinders freedom of expression online and State authorities have used technologies for the targeting and profiling of users to limit the right

538 Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far", *WIRED*, 3 December 2014, available at <http://www.wired.com/2014/12/sony-hack-what-we-know/>.

539 OHCHR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, 17 April 2013, UN Doc. A/HRC/23/40, para. 17, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

540 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 33, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

541 Freedom House, "Freedom on the Net 2014", available at <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VUczyJO5wg4>, accessed 4 May 2015

to freedom of expression. [542] Note that such user-targeting can happen at multiple levels, including at the governmental, private companies and infrastructural levels.

Meanwhile, a number of State authorities have made efforts to restrict the widespread use of technical tools, such as VPN technologies, or the Tor network, or other encryption and anonymity technologies. Users could otherwise employ these to circumvent filtering, blocking and/or accessing users' data. There have also been attempts to prescribe requirements for the disclosure of identity, and to press private companies in order to gain access to the service user's information for various purposes.[543]

According to Freedom House's report between May 2013 and May 2014, 41 countries passed or proposed legislation that enables or would enable: a) the penalization of legitimate forms of online speech; b) increases in governmental control over content; and/or c) expansions in governmental surveillance capacities. These laws also enable or would enable: a) the banning of online dissent; b) the criminalisation of online defamation; and c) the expansion of State regulators' powers, by broadening national security laws, blocking content in the absence of court orders, increasing intermediary liability, and conducting intrusive surveillance.[544] Also, according to the same report, blocking and filtering have been complemented by direct imprisonment of users to deter others and encourage self-censorship, to the point that more people were detained and prosecuted for digital activities in 2014 than ever before.[545]

Meanwhile, a report published by the Office of the UN High Commissioner for Human Rights clearly noted the general lack of procedural safeguards and the shortage of effective oversight in relation to the surveillance activities carried out. Moreover, the same report pointed out that attention is increasingly being given to mixed models of administrative, judicial and parliamentary oversight;[546] and effective remedies to the violation of the right to freedom of expression in online contexts are lacking.[547]

A number of other reports have also identified a general tendency for State authorities to impose on Internet intermediaries—e.g. ISPs, search engines and SNS Platforms—responsibilities regarding content and access control. In many cases these intermediaries have to bend to State pressure and law requirements to filter, block and control published online contents, as well as to provide personal data/information to State authority. Moreover, some States decline to recognize such intermediaries' limited liability, imposing criminal liabilities on them for objectionable content posted by third parties.[548] Thus, while Internet intermediaries are central to the protection of the rights to freedom of expression and privacy, many are under increasing pressure from State authorities, from around the

542 UNESCO, Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet, Report, 2015, Paris: UNESCO, pp. 36-39, available at <http://unesdoc.unesco.org/images/0023/002325/232563E.pdf>.

543 OHCHR, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, *Frank La Rue*, 17 April 2013, UN Doc. A/HRC/23/40, paras. 18-19, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40>.

544 Freedom House, "Freedom on the Net 2014", pp. 4-7, available at <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VUczyJO5wg4>, accessed 4 May 2015.

545 Ibid., pp. 1 and 7.

546 Pillay, "The Right to Privacy in the Digital Age", 12-13.

547 Ibid., 13-14.

548 Freedom House, "Freedom on the Net 2014", p. 6, available at <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VUczyJO5wg4>, accessed 4 May 2015.

globe, and end up acting in ways that fall short of international standards for legitimate limitations to these rights. [549]

Issues also persist regarding the extent to which societies respect the right to freedom of expression in online contexts as enjoyed by certain special social categories, such as women and members of the LGBTI community. Such groups, globally, still face socioeconomic and cultural barriers in accessing ICTs in the first place, and when they do overcome such barriers, they often become subject to increased risks of such illegalities as online harassment, threats and violence. In view of this, and given today's technical and other forms of capabilities—e.g. the avenues opened by PbD—it is clear that more can be done to achieve higher levels of respect towards the right to freedom of expression in online contexts. [550]

7.4 Balancing in concrete contexts

Balancing the right to freedom of expression and the right to privacy, especially in online contexts, is a challenge in the digital age. However, such an endeavour is facilitated by general principles and guidelines found in international human rights law and in regional and State case law. In online contexts, new balances must be reached through judicial deliberation of the many factors at stake, including consideration of new or altered factors that result from situational changes; e.g. from the advent of new technologies that "upset" previously accepted equilibria. Such deliberation will involve, amongst other tasks: a) the assignment of weight to each right; and b) the search for possible approaches to optimizing one right while avoiding or at least mitigating the compromise of the other right(s). In the following three sections, we discuss three scenarios that have received global attention in order to show how new balances were struck with respect to the rights to freedom of expression and privacy, in different judicial contexts.

7.4.1 The Google Spain Case

Google Spain is a landmark case in the EU that has achieved global influence due to the importance of the legal issue it addresses, and the judicial influences of the Court of Justice of the European Union (CJEU).[551]

Facts

The facts of the case are as follows:

In 1998 the Spanish newspaper *La Vanguardia* published two announcements in its printed edition regarding the forced sale of properties arising from social security debts. The announcements—of which the purpose was to attract as many bidders as possible—were

549 Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom, Report, 2014, Paris: UNESCO, pp. 19-20, available at <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

550 Demetrius Klitou, (2014) *Privacy-Invading Technologies and Privacy by Design*, Vol. 25, Information Technology and Law Series, The Hague: T.M.C. Asser Press, p. 272, available at <http://link.springer.com/10.1007/978-94-6265-026-8>..

551 ECJ, Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Judgment, 13 May 2014.

published on the order of the Spanish Ministry of Labour and Social Affairs, and later made available on the Internet.

One of the properties described in the newspaper announcements belonged to the plaintiff, whose name was included in the announcements. In November 2009, the plaintiff contacted the newspaper to complain that a Google search for his name led to the announcements, arguing that the data relating to him was no longer relevant because the forced sale had been concluded years before; and that such data should therefore be removed. The newspaper replied that erasing such data was not appropriate because the publication had been on the order of the Spanish Ministry of Labour and Social Affairs.

The plaintiff then contacted Google Spain in February 2010, asking that the links to the announcements be removed. Google Spain forwarded the request to Google Inc., whose registered office is in California, USA, taking the view that Google Inc. was the responsible body. The plaintiff subsequently lodged a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos, AEPD) asking both that the newspaper be required to remove the data; and that Google Spain or Google Inc. be required to remove the links to the data. On 30 July 2010, the Director of APED rejected the complaint against the newspaper but upheld the complaint against Google Spain and Google Inc., calling on them to remove the links complained of, and make access to the data impossible.

Google Spain and Google Inc. subsequently brought separate actions against the decision before the Audiencia Nacional (National High Court of Spain), basing their appeal on the following arguments:

Google Inc. was not within the scope of the EU Directive 95/46/EC (Data Protection Directive) and its subsidiary Google Spain was not responsible for the search engine;

There was no processing of personal data within the search function, and neither Google Inc. nor Google Spain could be regarded as a data controller in any event, thus the plaintiff—who would be the data subject—did not have the right to erasure of lawfully published material.

Outcomes

The outcomes and results from the case—which include the CJEU's delineation of new boundaries relating to the right to freedom of expression and the right to privacy— are, essentially, as follows:

An internet search engine operator is responsible—as a data controller—for the processing that it carries out of personal information which appears on web pages published by third parties. [552]

Based on the CJEU's interpretation of Article 4 Paragraph 1 under Directive 95/46/EC, the data controller's processing of personal data is considered carried out in the context of the activities of an establishment of the controller on the territory of a Member State; i.e. in this case in Spain, since Google Inc. has such representation in the EU Member state. [553]

Regarding the operations of intermediary search engine providers:

552 Ibid., para. 41.
553 Ibid., para. 60.

Data subjects in similar situations may now request "the information in question no longer to be made available to the general public" by a search engine.

The search engine operator must consider requests from individuals to remove such information—i.e. links between their names and freely accessible web pages resulting from a search on their name—including where the person's name or information is not erased beforehand or simultaneously from the web pages, and even, as the case may be, when the publication of the information in itself, on those pages, is lawful [554]; and remove such links where the search result(s) "appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed".

If the search engine rejects the request, the individual may take the case to relevant authorities, which may then order the removal of such links.

The decision aligns to the so-called right to be forgotten mooted in the proposed General Data Protection Regulation.

However, it can be noted that the Court did not explicitly grant such a right, depending instead on the data subject's rights deriving from Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union.

It ruled that the processing of personal data by the search engine operator is liable to "affect significantly the fundamental rights to privacy and to the protection of personal data", because the search result provided "a structured overview of the information relating to that individual, [...and thus it] concerns a vast number of aspects" of the plaintiff's life,[555] and because the links that Google identified between the plaintiff's name and the information in websites published by third parties were outdated and no longer relevant.

The Court also expressed that: "[the application] of Article 7(f) (Directive 95/46/EC) [...] necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (EU Charter of Fundamental Rights)". [556]

At the same time, the Court recognized that the individual's fundamental rights under Articles 7 and 8 of the Charter "override, as a rule, not only the economic interest to the operator of the search engine but also the interest of the general public in having access to that information upon a search". [557] It also recognised that the right to information access, in general, may—e.g. where the data subject would have played a role in public life, or if the access to the information is of preponderant interest to the general public—override the right to personal life and the right to personal data granted under the Charter's Articles 7 and 8.[558]

Thus, the new boundaries set by the CJEU may be characterised more generically by: a) the reshaping or extension of the duties and legal status of search engine providers like Google in EU jurisdictions; b) the exterritorial jurisdiction capacity of EU courts; c) the right of the

554 Ibid., para. 62.
555 Ibid., para. 80.
556 Italicized by authors, see Ibid., para. 74.
557 Ibid., para. 91.
558 Ibid.

plaintiff to protect his/her own data privacy in claiming a 'right to be forgotten' or more accurately a 'right to de-listing'; and d) the balancing of the right to privacy with other rights.

Consequences

The consequences of the case reach so far that they have not fully unfolded yet. Indeed, they may have much broader influences—which may be intended, unintended, direct or indirect—on both the industry and others' right to freedom of expression and information.

A Right to be Forgotten?

The practical applicability of a 'right to be forgotten' is also problematic. Though personal information will not be available after removing the links made by search engines in Europe, it will often remain possible to access the information even in its original location by other means, due to the openness and connectivity of the Internet, even if this is with some difficulty.

Who should balance the Rights?

In line with such views, some people argue that it is improper to "leave the search engines as intermediaries the task of deciding whether to delete information or not, based on vague, ambiguous and unhelpful criteria".[559] For instance, since it is difficult to draw clear lines on the points substantiating the Court's decision, the decision may cause fears from potential data privacy breach charges that lead to over-reaction by relevant intermediaries, and therefore to the inappropriate removal of non-privacy-invasive personal information, whether or not this would be directly related to persons' names.

Impact on smaller online service providers

The House of Lords commented that the judgement "does not take into account the effect the ruling will have on smaller search engines, which unlike Google, are unlikely to have the resources to process the thousands of removal requests they are likely to receive". [560] Similarly, Small and Medium enterprises (SMEs)—which are more likely than their giant counterparts to want to prevent potential legal controversies—may be more susceptible to fears that may arise due to the difficulties in the drawing of clear lines on the points substantiating the Court's decision; e.g. in balancing an individual's right to privacy with others' right to freedom of expression, thus risking that they overreact.

Impact on other types of intermediaries

The extension of this ruling to other types of intermediaries is not excluded. The guidelines provided by the Article 29 Data Protection Working Party regarding the application of the verdict, published recently, indicate that it is possible that the verdict would be applied

559 House of Lords, *House of Lords - EU Data Protection Law: A "Right to Be Forgotten"? - European Union Committee*, 23 July 2014, available at <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.

560 Ibid.

to other intermediaries whenever the conditions established in the ruling are met. [561] Additionally, Article 29, the association of Data Protection Authorities of EU Member States, whose opinions have soft law status, has called for an extension of the de-listing requirement to all Internet domains—including the '.com' domain—for a satisfactory guarantee of the rights of data subjects. This measure is problematic in legal realities, insofar as it suggests the imposition of European jurisprudence on Internet users from countries outside the EU. A different option is to compel Google.com to provide a specific version of its search results for users accessing it from EU-based domains. Taking the measure to an extreme, on a global basis, each country could then end up with a fragmented but distinct experience of the Internet even when using the same Internet services.

Impact on the Rights to Freedom of Expression and Information

The decision may also lead to an undesired chilling effect on the right to freedom of expression and the right to information of others. Firstly, it seems especially paradoxical where it would impose an obligation on the intermediary to remove links in cases where the original information published on third party websites is both deemed legal and not removed, as is the situation in the Google Spain case. Secondly, one commentator—who pointed out that in international human rights law "there is no right to be forgotten", has argued that the decision indicates that Europe may have unintentionally established a new right to "censor some information that you don't like". [562] The commentator also contended that one of the main drawbacks of the decision is that it may lead to the privatization of censorship, insofar as the decision may now sanction search engines to censor personal data upon requests from individual data subjects, independently of further court decision-making.

Indeed, it may be argued that while it is still unclear how effective the Google Spain case is in terms of practical privacy protection, even though it has set new boundaries and extended the legal rights, it is clear that it has eroded the right "to receive and impart information and ideas without interference by public authority and regardless of frontiers".[563] While the CJEU has made the decision in favour of data privacy in this leading case to make it clear that a European citizen can choose to be delisted—at least on parts of the Internet under the EU jurisdiction, when the information disclosed online regarding the citizen's past is deemed to be of no public interest—this might have severe repercussions on the wider rights to information online and expression. The academic Jonathan Zittrain has suggested that a 'right to reply' could have provided a better balance than that struck by the Court.[564]

561 Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos(AEPD) and Mario Costeja González" C-131/12, 2014, para. 17, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-1>.

562 Natasha Lomas, "Jimmy Wales Blasts Europe's 'Right To Be Forgotten' Ruling As A 'Terrible Danger", *TechCrunch*, 7 June 2014, available at <http://techcrunch.com/2014/06/07/wales-on-right-to-be-forgotten/>.

563 Article 11, EU Charter of Fundamental Rights.

564 See J. Zittrain, "Don't Force Google to 'Forget", *New York Times*, 14 May 2014, available at <http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0>.

7.4.2 Privacy of public figures and protection of freedom of expression

Although public figures and public celebrities differ in whether being appointed to public office, both occupy special social status and thus exert more influence than ordinary people in a community. According to the definition by the Council of Europe, public figures are persons who hold public office and/or use public resources and, broadly speaking, include all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain.[565] It is also recognised that the special status of public figures comes at the price of compromises to their rights to reputation and privacy, to an extent; [566] and, in cases of conflict, priority to others' right to freedom of speech and right to information, before law.

Prosser provided partial explanations on the rationales underpinning this legal doctrine in the USA legal context. First, he suggests that since most public figures seek publicity willingly, they cannot complain of being monitored and talked about. Second, public figures' personalities and affairs have already become public and no longer can be regarded as private business. Third, public figures occupy a special social status and are thus in a better position than most ordinary people to respond to defamatory statements.[567] In USA law, the public figure privilege doctrine is a well-established doctrine in privacy law for the publicity tort by 1964,[568] and was recognized in the landmark *Sullivan* libel case.[569]

While the public interest threshold counts in general, according to the Gertz doctrine[570] public figures include three categories of persons: a) public officials; b) those voluntarily playing prominent roles in specific public controversies; and c) all-purpose public figures. The terms representing the first two categories are self-explanatory. The third category—i.e. 'all-purpose pubic figures'—refers to those whose names are a household word, normally having prominent positions, persuasive power and influence. Additionally, similar to the second category, there are involuntary public figures who "simply [find themselves] at the centre of important societal events" and could in certain circumstances "be thrust into the role of a public figure".[571]

Though the public figure doctrine has not been adopted explicitly by the US Supreme Court in constitutional analyses of privacy cases, it has always played a major role in the common law of privacy. For instance, the Court has used the doctrine in the context of individuals' right to information privacy against the government.[572]

---

565 Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the Right to Privacy, n.d., para. 7, available at <http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm>.

566 William L. Prosser, "Privacy", (1960) *California Law Review*, Vol. 48, No. 3, p. 411.

567 Ibid., pp. 410-411.

568 Catherine Hancock, "Origins of the Public Figure Doctrine in First Amendment Defamation Law", (2006) *New York Law School Law Review*, No. 1, pp. 87-88.

569 New York Times co. v. Sullivan, 376 U.S. 254 (1964).

570 See a discussion of the case the related legal doctrine at: James C. Mitchell, "The Accidental Purist: Reclaiming the Gertz All Purpose Public Figure Doctrine in the Age of 'Celebrity Journalism'", (2002) *Loyola of Los Angeles Entertainment Law Review*, Vol. 22, pp. 559-581.

571 Nathaniel Jurist Gleicher, "John Doe Subpoenas: Toward a Consistent Legal Standard", (2008) *Yale Law Journal,* Vol. 118, No. 320, p. 118, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1378742>.

572 Susan M. Gilles, "Public Plaintiffs and Private Facts: Should the 'Public Figure' Doctrine Be Transplanted into Privacy Law?", (2005) *Nebraska Law Review*, Vol. 83, No. 4, pp. 1205 and 1212.

Other jurisdictions adopt different, and at times substantially distinct, approaches to protecting freedom of expression. For instance, while Japanese law accepts the public figure doctrine, it limits the scope to a very small number of individuals who hold significantly prominent positions—e.g. top corporate executives and leading politicians—and thus are able to substantially affect society.[573] In German law, public figures are clearly distinguished from private ones and organised in three categories, each granted a different type of protection: a) permanent public figures; b) celebrity public figures; and c) temporary public figures.[574]

The European Court of Human Rights (ECtHR) follows a more elaborated approach towards the protection of the privacy of public figures in its case law. It refers to a public interest test involved, in combination with the distinction between public and private figures. It also considers the nature of the publicized information, such as: a) whether the information is of legitimate interest to the public;[575] b) the formality and methodologies of the publication;[576] c) the proportionality of the interference measures;[577] d) the location of the published images; and e) the style of the expression. [578]In *Hachette Filipacchi Associes v. France*, the Court used more concrete criteria to achieve a balance in a conflict between the two rights, which included, amongst others: the measures and veracity of the information taken; contribution to a debate of general interest; official functions; and the nature of the person and the subject's public profile. [579]

In the digital age, the Court is cautious in restricting online publication. The case *Mosley v. the United Kingdom* concerns the online publication of Internet content that has attracted a large audience. Albeit the disclosed matter is of a purely private nature, of limited public interest, and although the information was published mostly for entertainment purposes, the Court unanimously rejected the plaintiff's complaint regarding the absence of a legal requirement to give individuals notice before publishing materials regarding their private life.[580]

The Court has made several decisions relating to the balance between the right to freedom of expression and the right to privacy (closely related to reputation) in online contexts (including online publication), and it still strives to clarify new legal issues and to seek balances between the two rights. On the one hand, it has emphasized the importance of the communicative and vast storage capabilities enabled by the Internet, as well as affirming that freedom of expression under Article 10 of the ECHR still applies online. On the other hand, it has also paid attention to the special character of the Internet and the differences between the online and the offline worlds.

The recent case law report by the Court revealed such changes, by deciding, for instance, that once private or personal information such as a person's identity and name is online, the need to protect its confidentiality will no longer constitute an overriding requirement.

---

573 Scott. J. Shackelford, "Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures", (2012) *American Business Law Journal*, Vol. 49, No. 1, p. 5.

574 Ibid., Section V.

575 ECtHR, *Von Hannover v. Germany*, Judgment, 24 June 2004, Application No. 59320/00.

576 ECtHR, *Sapan v. Turkey*, Judgment, 8 June 2010, Application No. 44102/04.

577 ECtHR, *Hachette Filipacchi Associes v. France,* Judgment, 14 June 2007, Application No. 71111/01.

578 ECTHR, Lillo-Stenberg and Saether V. Norway, Judgment, 16 January 2014, Application No. 13258/09.

579 ECtHR, *Hachette Filipacchi Associes v. France,* Judgment, 14 June 2007, Application No. 71111/01. (The case is still pending before the Grand Chamber after a recent hearing in April 2015) See also a discussion at Section 6.4.

580 ECtHR, *Mosley v. the United Kingdom,* Judgment, 10 May 2011, Application No. 48009/08.

The Court, however, has also considered the amplifying effect of the Internet which affects its specific balance between the protection of freedom of expression and respect for other rights. This is reflected in the Court's strong support for protecting minors and children by national laws; the press' responsibility not to air details of an individual's private or family life which are available online, but not falling within the scope of any public or political debate on a matter of general importance; journalists' responsibility to be extended to publications outside their employer's website, but in their names; and the exemption of public figures from public pressure on account of cases concerning a member of his or her family, even if the related data is accessible on the Internet; as well as higher level of protection of political, militant and polemical expressions on the Internet. [581]

The Court's exploration of the boundaries of the rights to freedom of expression and privacy will continue, especially where they conflict with each other or with other rights and values. One issue is the legal responsibilities of intermediaries on disclosure of private information without the consent of information subjects, and defamatory comments that are not controlled by them. In the most recent *Delfi AS v. Estonia*, the Court has favoured the plaintiff (in the capacity of data subject) by placing more responsibilities on the Intermediaries.[582] The ruling has effectively treated the particular platform as a form of media rather than an intermediary, and ruled that Delfi had a duty to pre-moderate content prior to its publication, rejecting the defence that the company had removed the offending content once it had been notified. This decision has serious consequences for, and could chill both freedom of expression and the right to information in online contexts. By requiring a form of prior restraint, it has seemingly weighed on the definitional side of balancing the two rights, which removes the flexibility of ad hoc balancing. In a subsequent case[583], the Court produced a further opinion, deciding against imposing civil liability on website operators for third-party content, explaining that this was different from the Delfi case because the comments concerned did not include hate speech.

7.4.3 Anti-terrorism legislation and privacy protection

As human societies are subjected to changes, such as those in the nature of pressing terrorist attacks and other security threats, they are continuously challenged to re-balance or re-coordinate the right to individual privacy and the right to public security. For instance, while mass- and targeted-surveillance are often justified in most countries based on reasons of public security, privacy protection is often seen to become compromised by quick legislation that justifies bulk surveillance measures, supposedly used to detect potential terrorists. And in this political climate characterised by terrorism and counter-terrorism, both domestically and in other jurisdictions, the relevant laws are increasingly permissive. For instance, often they authorise intelligence services to intercept communications—e.g. phone and email communications—in the absence of a judge's approval. In other cases, such as Apple and the USA's Federal Bureau of Investigation, the debate was sometimes framed as (individual data) security versus (national) security; and sometimes as an attempt by the authorities to interfere with "freedom of speech" in the mode of compelling "code as speech". These examples point to some of the complexities involved.

581 ECtHR, "Council of Europe: European Court of Human Rights, Internet: Case-Law of the European Court of Human Rights", June 2011, pp. 6-16, available at <http://www.refworld.org/docid/4ee1d5bf1a.html>, accessed 9 September 2015.

582 ECtHR, *Delfi AS v. Estonia,* Judgment, 16 June 2015, Application No. 64569/09, para. 158.

583 Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, Application No. 22947/13, European Court of Human Rights, 2016

A 2012 UNODC report mentioned several uses of the Internet in terrorist activities, including as a propaganda tool, including for the incitement, recruitment and radicalization of individuals or groups of individuals; and as a means of cyberwarfare, including by enabling the financing, planning and execution of cyber-attacks.[584] Thus it is clear that counter-terrorism controls in cyberspace become useful. However, there are costs attached to such controls. Firstly, unless such controls are framed in adequate systems that follow legal requirements, and in particular the principles of proportionality and necessity, it would be reasonable to raise rule of law concerns and international standards in the first instance. Secondly, as pointed out in the same report, counter-terrorism initiatives relating to the use of the Internet can influence the enjoyment of a range of human rights, including the rights to freedom of speech, freedom of association, privacy and fair trial.[585]

The most frequently-raised issue is not with the collection and/or analysis of data that pertains to targeted suspects; but rather with the collection and analysis of data and metadata for "potentially suspicious behaviour". The latter may threaten the privacy of each citizen by subjecting them to behavioural pattern analyses that violate the presumption of their innocence. The proportionality of such bulk surveillance measure, in general, is debatable in practice. As pointed out in the report issued by the UN Human Rights Council on the Right to Privacy in the Digital Age: "It will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened".[586]

The large-scale sharing of databases among State agencies—including Law Enforcement Agencies —can present issues, too. For instance, it can involve, amongst other irregularities: unauthorised changes in the purpose(s) underpinning the analysis of the data; the abuse or misuse of the shared data; and the circumvention of court orders by direct request for the access of data stored within the systems of private companies. These potential risks to data privacy require such anti-terrorism laws to be under some effective oversight, to be limited by procedural safeguards, as well as to be effectively remedied via proper legal procedures.[587] Within this context, transparency, amongst other tools, may be used, to satisfy the public that adequate balances are achieved between privacy and security, and that there is no excessive erosion of the essence of the right to privacy. Transparency can also help to establish trust in the claim that any limits on privacy are only exerted for genuine security purposes, and exclude reasons that exist outside the international standards, such as narrow political advantage.

Usually, surveillance and law enforcement agencies have been eager to gain access to the wide range of personal information available from information systems created for a variety of purposes, including ones completely unrelated to public security.[588] However, it is valuable to consider instruments like the 'TheNecessaryandProportionate.org principles' in order ensure the maintenance of a balance within the larger framework of human rights.

---

584 UNODC, *The Use of the Internet for Terrorist Purposes*, Report, September 2012, Vienna: United Nations, pp. 3-13, available at <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>.

585 Ibid., p. 13.

586 Pillay, "The Right to Privacy in the Digital Age", 9.

587 Ibid., 11-14.

588 Douwe Korff and Ian Brown, The Use of the Internet and Related Services, Private Life and Data Protection: Trends and Technologies, Threats and Implications, Report, Council of Europe, March 2013, p. 15, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/use-Internet-and-related-services-private-life-and-data-protection-trends-and-technologies>.

CHAPTER 8 Bridging the gaps: new tendencies in policy and law

8.1 Introduction: the shifting power of multiple players

On the whole, the rights to freedom of expression and privacy on the Internet can be assessed to be facing new threats. There have been significant evolutions in Internet ecosystems in the past years, including in how state authorities, giant ICT service providers and intermediaries (hereafter referred to as 'service providers'), Internet users and civil society organisations engage with the Internet. Indeed, globally, governments play a larger role in the online environment, enormous service providers control the majority market share,[589] and more and more Internet users come to rely on an evolving range of services. These and other factors contribute to constant and evolving threats to privacy, freedom of expression and other values and rights in the online context.

State authorities

On the one hand, the increasing power that is gained by State authorities can enable the protection of the rights and values discussed in this Report, including privacy, freedom of expression, freedom of information and transparency. For instance, increasingly, new and updated legislation for the protection of data privacy and security enhances protections—against data abuses and misuses by private individuals and the private sector, as well as against terrorist attacks, cybercrime and cyber-attacks—and prevent actions that could stifle and downright threaten desired values and rights. On the other hand, increases in the State's involvement, including by means of similar legislation, can be exploited to weaken the same rights and values.

Service providers

The service providers' engagement in private censorship and/or cooperation relating to secret mass surveillance programs can contribute to increasing public distrust, harming the same service providers. To address such distrust, the service providers have made efforts to build up internal and external transparency that helps them protect privacy and freedom of expression, including by fending off the pressures from State authority.

However, given that data constitutes the "oil" of the information economy, it is reasonable to expect more and more business models that would depend on the collection, storage and processing of personal data, and this may continue to contribute to further erosion and stifling of the rights and values discussed in this report, including in online contexts. Additionally, as data security and encryption may be or become drawcards and components of existing and upcoming business models, such models and the said technologies (including cryptographic and security technologies) depend largely on technology innovations that may die out because of stricter regulation and/or over-regulation. All this places the service providers in an ambiguous situation, which is compounded by transnational operations.

589 According to DeNadis, greater privatization of Internet Governance in some circumstances will be an invitation for greater government regulation. See Laura DeNardis, "The Privatization of Internet Governance", Yale Information Society Project, Working Paper Draft, September 2010, p. 11, available at <http://api.ning.com/files/8q30Xud1XrmD6Sd5rOiSolcw3agdQi5NNoWZrQGmOIpKc0fdqfKN0Ax5Z8ZypNexdCwBicqDKcADrRU5hs4ZQjBy0RPTg BmK/DENARDISThePrivitizationofInternetGovernance.pdf>, accessed 17 September 2015.

Internet users

While the rights of individual Internet users should lie at the core of the evolution of the Internet eco-systems, they are the most vulnerable to challenges and threats, not only in the senses already discussed in this Report but also due to several other factors. For instance, many Internet users (and therefore their rights) are vulnerable to the 'privacy for service' trade-off in online contexts, for many reasons, which include human tendencies for immediate gratification; and a lack of understanding and/or avoidance with respect to such complex notions as the operationalisation of the right and value of privacy in novel and evolving online contexts. Other users may understand or believe—whether substantially autonomously or not—that privacy is not substantial enough as an independent value for practical interest, possibly claiming a lack of concern relating to privacy breaches, based on the (often publicised) view that one should "have nothing to hide".

Additionally, as a result of such weaknesses and other factors, few users are willing to read through the privacy clauses provided by the Service Providers in the relevant terms of service, and those willing to do so will normally find it difficult to do it consistently (e.g. to check for any changes in the terms) and/or to understand what they read. In general, it is currently widely recognised that individual private users are the weakest players in Internet eco-systems, that such weakness is already exploited, and that there is potential for significant increases in such vulnerabilities and the corresponding threats and potential impacts. It is therefore reasonable to call for more protection from State authorities, especially against the abuse and misuse of the users' personal information,[590] including, if not primarily, by means of regulatory safeguards and judicial oversight.

Civil society organisations

Civil society organizations also play an important role in Internet eco-systems, mitigating some of the threats. Their main role is to represent the public interest in regard to Internet users, and to actively participate in the making of Internet governance policy and law. For instance, after the Snowden revelations, civil society was prominent in promoting increased awareness, resorting to legal remedies and initiating Internet freedom campaigns.[591] International organizations—including several types of Internet governance organizations, whether commercial or NGOs—play a similar and equally important role. These include such influential organisations, corporations' initiatives and groups as the Global Network Initiative (GNI); the Telecoms Dialogue; the Internet Corporation for Assigned Names and Numbers (ICCANN); the Internet Engineering Task Force (IETF); the United Nations-sponsored World Summit on the Information Society (WSIS); the Internet Architecture Board (IAB); the International Telecommunications Union (ITU); the Working Group on Internet Governance (WGIG); and the Internet Governance Forum.[592]The Global Alliance for Media and Information Literacy seeks to empower users with competencies necessary to counter threats and protect rights.

590 Although this does not mean that in many countries state authorities are more predatory. See Anita Allen, (2011) *Unpopular Privacy: What Must We Hide?*, Oxford, New York: Oxford University Press.

591 Freedom House, "Freedom on the Net 2014", p. 12, available at <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VUczyJO5wg4>, accessed 4 May 2015

592 For their specific roles in Internet governance, see Jovan Kurbalija, (2014) *An Introduction to Internet Governance*, Sixth Edition, Msida and Geneva: DiploFoundation, available at <http://www.diplomacy.edu/resources/books/introduction-Internet-governance>; Lee A. Bygrave and Jon Bing, (2009) *Internet Governance Infrastructure and Institutions*, Oxford: Oxford University Press.

8.2 New policy developments on online privacy protection

The common belief in the post-Snowden world is that Internet users, and the public in general, should be protected against wrongful surveillance activities, including by providing more transparency regarding mass-surveillance activities, and by enhanced scrutiny of the laws and policies that regulate these activities.

The problem is starting to be addressed to some extent, in various locations around the globe. In January 2014, the President of the USA called for an end to the NSA's bulk surveillance on individuals.[593] Later in the same month, the Department of Justice relaxed restrictions on the public disclosure of the Foreign Intelligence Surveillance Act (FISA), as well as on the disclosure of orders and National Security Letters. The White House also proposed laws to restrict the NSA's collection of bulk-calling records, with the proposal being received favourably.

The USA government has also released a six-year-old report on the NSA's once-secret programme, which involved the collection of information on American citizens' calls and emails.[594] On 7 May 2015, a federal appeals court in the US ruled, in a landmark decision, that the bulk collection of telephone metadata that had occurred was unlawful, clearing the way for a full legal challenge against the NSA.[595] The US has also been considering to improve transparency by a truly uniform federal standard for the notification of breaches.[596]

In Europe, a UK tribunal ruled that the regime governing the sharing of electronic communications between Britain and the USA, which were intercepted in bulk, was unlawful until last year.[597] Likewise, the EU parliament declared the mass surveillance in some Member States in cooperation with the NSA illegal.[598] Also, the EU has taken steps on privacy and data protection, by means of the ECJ's invalidating of data retention law,[599] and clarified the house-hold exemption scope in CCTV use.[600] Other efforts in this region include: a) the increased enforcement of EU Data Protection Rules across the EU; b) the revision of the Safe Harbour Program and debate around the "Privacy Shield" replacement; and c) the ECJ's scrutinizing of the Passenger Name Records (PNR) exchange under EU's data protection principles.[601]

---

593 "Transcript of President Obama's Jan. 17 Speech on NSA Reforms", *The Washington Post*, 17 January 2014, available at <http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html>.

594 "White House Releases Report on NSA Surveillance Six Years Later", *The Guardian*, available at <http://www.theguardian.com/world/2015/apr/25/nsa-surveillance-report-white-house-releases-six-years-later>, accessed 16 May 2015.

595 Devlin Barrett and Damian Paletta, "NSA Phone Program Is Illegal, Appeals Court Rules," *Wall Street Journal*, 7 May 2015, sec. US, available at <http://www.wsj.com/articles/appeals-court-rules-nsa-phone-program-not-authorized-by-patriot-act-1431005482>.

596 "Data Security/Breach Notification | U.S. Chamber of Commerce", 23 April 2015, available at <https://www.uschamber.com/issue-brief/data-securitybreach-notification>.

597 Owen Bowcott and Legal Affairs Correspondent, "UK-US Surveillance Regime Was Unlawful 'for Seven Years'", *The Guardian*, available at <http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-Internet-surveillance-unlawful-court-nsa>, accessed 16 May 2015.

598 "US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Impact on EU Citizens' Fundamental Rights - P7_TA-PROV(2014)0230", March 2014, available at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230>.

599 ECJ, Joined cases C-293/12 Digital Rights Ireland Ltd v. Minister for Communications and Others and C-594-12 Kärntner Landesregierung and Others, Judgment, 8 April 2014.

600 ECJ, Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, Judgment, 11 December 2014.

601 Dan Cooper and Maria-Martina Yalamova, "Top 10 International Privacy Developments of 2014", *InsidePrivacy.com*, 4 February 2015, <http://www.insideprivacy.com/international/european-union/top-10-international-privacy-developments-of-2014/>.

Additionally, new data protection legislation has been gaining momentum across the globe. The EU is in the process of adopting a new data protection package, moving its old data protection mechanisms into the digital age. In the USA, in February 2015, the White House released its draft of the Consumer Privacy Bill of Rights.[602] More generally, the number of countries updating previous data protection laws or adopting new ones—i.e. including, amongst others, Singapore, Australia, Brazil (Data Privacy Bill & Marco Civil da Internet or the "Internet Law"), South Africa, Turkey and Chile—continued to grow throughout 2014.[603]

Moreover, the USA and Canadian Supreme Courts have, in three recent verdicts, restricted access to law enforcement to personal data on smartphones, with respect to searches incidental to an arrest, with the former recognizing the importance of modern smartphones as devices containing rich personal information. [604] The latter ruled that while "[i]nformational privacy is often equated with secrecy or confidentiality, and also includes the related but wider notion of control over, access to and use of information[,]particularly important in the context of Internet usage is the understanding of privacy as anonymity".[605] It has also judged that: a) while such searches in the absence of a warrant are allowed consequent to an arrest, the searches are limited by detailed legal restrictions and requirements; and b) record-keeping is required for later judicial review.[606]

The UN Human Rights Council too has made efforts to curtail mass surveillance and protect online privacy. In addition to its past comment on privacy,[607] a new Special Rapporteur was appointed in July 2015[608] and a resolution was passed on the Right to Privacy in the digital age by the General Assembly, strongly affirming the core status of privacy in human freedom.[609] Likewise, UNESCO has made continuous efforts in multiple events, investigating the impacts of ICTs on the right to privacy and contributing to better online privacy, access, trust and transparency.

As previously mentioned in this report, some private sector organisations have already taken initiatives against mass surveillance by publishing transparency reports that disclose information about requests they receive for access to personal data by USA- and EU-based national authorities. Some mobile companies—e.g. EE, O2 and Three—also took legal action against government agencies which made such requests. Others have rejected requests to cooperate, e.g. Apple's refusal to compromise default end-to-end encryption within its device OS (operating system), leading to critiques from intelligence services

602 Libbie Canter, "White House Privacy Bill: A Deeper Dive", *Insideprivacy*, 27 February 2015, available at <http://www.insideprivacy.com/advertising-marketing/white-house-privacy-bill-a-deeper-dive/>.

603 Dan Cooper and Maria-Martina Yalamova, "Top 10 International Privacy Developments of 2014", *InsidePrivacy.com*, 4 February 2015, <http://www.insideprivacy.com/international/european-union/top-10-international-privacy-developments-of-2014/>.

604 United States Supreme Court, *Riley v. California 573 U.S.* (2014), paras. 21 and 17, available at <https://supreme.justia.com/cases/federal/us/573/13-132/>, accessed 17 May 2015

605 Supreme Court of Canada, *R. v. Spencer,* 2014 SCC 43, 214.

606 Supreme Court of Canada, *R. v. Fearon*, 2014 SCC 77, [2014] S.C.R. 621 (2014), 623.

607 OHCHR, CCPR General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), 8 April 1988, UN Doc. HRI/GEN/1/Rev.9 (Vol. I), para. 1, available at <http://www.refworld.org/docid/453883f922.html>, accessed 29 May 2015.

608 Disclosure: the lead author of this report, Prof. Joseph A. Cannataci, was appointed as the Rapporteur. He and his team were commissioned for this research before his appointment.

609 "Resolution Adopted by the General Assembly on 18 December 2013 [on the Report of the Third Committee (A/68/456/Add.2)] 68/167. The Right to Privacy in the Digital Age", December 2013, available at <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167>.

agencies.[610] Other companies—like Google, Microsoft and Apple—have started to build local data centres, to store their consumers' data within the consumers' own homeland jurisdictions, and thus follow local law and avoid further judicial conflicts; ultimately gaining consumer trust.

Also, private sector organisations have made initiatives to negotiate and start industrial standards. For instance, the Global Network Initiative (GNI) has published a report titled *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, which recommends that States collaborate in creating a secure electronic system that involves the use of multiple resources for the management of Mutual Legal Assistance (MLA) requests.[611] Similarly, the USA's Digital Advertising Alliance (DAA), a consortium of the nation's largest media and marketing associations, has established self-regulatory standards for online advertising, and was to commence enforcement of the Application of Self-Regulatory Principles to the Mobile Environment (DAA Mobile Guidance) on September 1, 2015.[612]

The contribution of civil society organizations has included legal cases against the misuse and abuse of data from both public bodies[613] and private companies. Possibly even more significant, users are more active in bringing class suits against digital giants to protect their own data privacy. In the *Vidal-Hall et al v Google* judgment, in March 2015, the UK Court of Appeal classified the misuse of private information as a tort, which implies that claimants are now, under the U.K.'s Data Protection Act of 1998, able to recover damages for non-material loss.[614]

It is clear that in the past few years the protection of privacy, as well as its balancing with other values and rights, has become a major issue.

8.3 Freedom of expression: still a long way to go

Globally, the threats to freedom of expression differ from those endangering the right to privacy (and to reputation), at different levels. One key threat to the former is the disproportionate impinging by the latter. For instance, the *Google Spain* decision risks leading to such repercussions as the privatisation of censorship. Similarly, there are considerable threats to freedom of expression from defamation law, and in particular from criminal defamation law. For example, according to a recent report, criminal defamation laws in the EU threaten freedom of expression—favouring public figures, and especially public officials.[615] Thus it is useful to remark that while there are legitimate limitations to both rights under national and international law, this threat to freedom of expression may

610 Institute for Human Rights and Business, "ICT, Human Rights & Business: A Roundup of 2014 and Challenges for 2015", 12 January 2015, available at <http://www.ihrb.org/commentary/ict-human-rights-business-roundup-2014.html>, accessed 16 May 2015.

611 Global Network Initiative, "Data Beyond Borders: Mutual Legal Assistance in the Internet Era | Global Network Initiative", available at <https://www.globalnetworkinitiative.org/content/data-beyond-borders-mutual-legal-assistance-Internet-era>, accessed 16 May 2015.

612 Morgan Kennedy, "Digital Advertising Alliance Will Begin Enforcing Its Mobile Guidance September 1, 2015", *InsidePrivacy.com*, 14 May 2015, available at <http://www.insideprivacy.com/advertising-marketing/digital-advertising-alliance-will-begin-enforcing-its-mobile-guidance-september-1-2015/>.

613 ECJ, Joined cases C-293/12 Digital Rights Ireland Ltd v. Minister for Communications and Others and C-594-12 Kärntner Landesregierung and Others, Judgment, 8 April 2014.

614 Judith Vidal-Hall, "Judith Vidal-Hall: Taking on the Giant - Index on Censorship", *indexoncensorship.org*, 22 April 2015, available at <https://www.indexoncensorship.org/2015/04/judith-vidal-hall-taking-on-the-giant/>.

615 International Press Institute, *Out of Balance: Defamation Law in the EU and Its Effect on Press Freedom*, Report, July 2014, available at <http://www.freemedia.at/ecpm/defamation-law-report.html>.

only be kept at bay if the balancing that occurs between freedom of expression and other rights (including that to privacy) strives to preserve the essence of the right.

Another major threat to freedom of expression is the arbitrary cut-off, blocking, filtering and censorship in the name of national security or anti-terrorism. While it is possible to justify such restrictions,[616] as well as limitations on the right to information,[617] the risk is that such restrictions and limitations would exceed the thresholds of necessity and proportionality; and will be used illegitimately, e.g. for a ruling party's political advantage. Such risk may be heightened in the absence of such control measures as procedural protection of the suspects, and continuation of mass surveillance measures that target all related data subjects and official transparency.[618] In general, then, there should be sufficient legal safeguards to cope with the risks and challenges that arise from the merging of the use of data (including personal data) for law enforcement, national security and intelligence service purposes.[619]

In several countries, violations of offline rights to free expression are carried over to online. To implement this, there are often direct liability conditions that are imposed on Internet intermediaries for access and content control, and threats to de-register or fine them. There are also actors who attack online expression with tactics like DDoS assaults and x infections.

Freedom of expression has also made some gains against overly broad restrictions. For instance, the Indian Supreme Court found a legal provision, which had criminalized the posting of menacing or grossly offensive information, as both unconstitutional and a restriction to the right to freedom of speech.[620] Similarly, a number of States are realising the dangers and difficulties of limiting online expression, and beginning to embrace Media and Information Literacy as a means to avoid a paradigm of *protecting* citizens from illegitimate content online, and instead to focus on the *preparation* of the users with the knowledge and skills required to take a rights-led approach in engaging effectively in the online world.

616 In the sense of blocking related websites. Hayley Richardson, "France to Debate 'Frighteningly Intrusive' Surveillance Powers", *Newsweek*, 20 March 2015, available at <http://europe.newsweek.com/france-debate-frighteningly-intrusive-surveillance-powers-315507>.

617 Alissa J. Rubin, "Lawmakers in France Move to Vastly Expand Surveillance", *The New York Times*, 5 May 2015, available at <http://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html>.

618 Jonida Milaj and Jeanne P. Mifsud Bonnici, "Unwitting Subjects of Surveillance and the Presumption of Innocence", (2014) *Computer Law & Security Review*, Vol. 30, No. 4.

619 See Cannataci's detailed analysis of data sharing by both sectors in Europe: Joseph A. Cannataci, "Defying the Logic, Forgetting the Facts: The New European Proposal for Data Protection in the Police Sector", (2013) *European Journal of Law and Technology*, Vol. 4, No. 2, Sections 2.8 and 2.9, available at <http://ejlt.org//article/view/284>.

620 Jason Burke in Delhi, "India Supreme Court Strikes down Internet Censorship Law", *The Guardian*, available at <http://www.theguardian.com/world/2015/mar/24/india-supreme-court-strikes-down-Internet-censorship-law>, accessed 17 May 2015.

CHAPTER 9 Conclusions and recommendations

9.1 Introduction

In the previous Chapters, this Report has analysed the main issues relating to the rights and values of privacy, freedom of expression and information, and transparency, and addressed key challenges revolving around the balancing of these rights and values in the digital age. It has also illustrated challenges to the rights of privacy and freedom of expression—especially those linked to individuals and the online context—as may be expected to escalate in the near future due to fast advances in the ICTs. The Report has also illustrated how the interplay and interactions between multiple players—e.g. the State agents, Internet users, ICT companies, civil society organizations, the judiciary and the security services—shapes the rights to freedom of expression and privacy online, as well as the nature of the protection mechanisms adopted in relation to such rights.

- **Traditional laws and regulations do not transpose seamlessly to the online world**

As revealed by a review of the *status quo* in the previous Chapters, traditional laws and regulations for the protection of privacy and freedom of expression—as formulated in the pre-digital era to reflect behavioural boundaries in communal life—cannot be applied seamlessly to the current and upcoming online world. Instead, in many cases, updated and/or new laws and regulations are required in order to prescribe and/or support protection mechanisms for these rights, which apply to the current (and upcoming) situations. This is especially true in view of the pressing privacy threats that result in the digital age from such existing and evolving phenomena as: the increasing cross-border data transfers; all sorts of mass surveillance practices; the rise of Cloud computing, along with such other technologies as distributed and grid computing; the growing use of drones and smart devices; and the advent of big data technologies.

The need for novel and updated laws and regulations is also clearly visible in view of the growing threats to freedom of expression. Indeed, State and non-State actors are gaining massive capacities in the control of the use of the Internet, especially as equipped with multiple new technologies for the purposes of censoring, filtering, blocking and attacking information and information services, by means of such technologies as: a) DPI; b) packet filtering; c) Domain Name System (DNS) filtering and redirection; d) Internet address blocking; e) denial of service attacks; f) portal censorship and search result removal; g) website take-down; h) network disconnection and connection reset; and i) control of Internet Exchange Points (IXPs). In many countries, these new technical measures and instruments have hardly been well-confined by domestic laws for freedom of speech and privacy. This is the case, in particular, when cybercrime and online terrorist activities are a major concern, or where the governments adopt approaches that involve tight political control.

- **How we can achieve more transparency and limits of transparency**

As showcased in the UNESCO's Internet Freedom Series[621] and other research reports, transparency—as a communal value—can be achieved by protecting the individual's

621 UNESCO Series on Internet Freedom: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/publications-by-series/unesco-series-on-internet-freedom/

rights to freedom of expression and information. In turn, transparency can also support the same two rights. However, since the disclosure of personal information may—directly or otherwise—influence others' private lives and public image, transparency and the right to expression, including the right to information can also be restricted by other individuals' exercising of their rights to privacy (and reputation). This is particularly the case in online contexts, which are characterised by the ability to publish digitised personal information.

- **Traditional technical and legal mechanisms do not suffice**

Against the above background, traditional technical and/or legal mechanisms do not suffice in coping with the escalating online challenges to the rights to privacy and freedom of expression and transparency. There are, however, many recent developments in Internet Governance to enhance them at the international and domestic stages.

- **Industry and State governments appreciate the value of transparency**

The growing need for transparency is nowadays clearly visible to both the industry sector and State governments, who recognise its value in enabling the clear definition of rules and procedures for the protection of privacy and freedom of expression. In addition, multiple international organizations—including UNESCO and various NGOs—are paying more attention to the protection of online human rights and have published a series of research reports. Similarly, States across the globe have proposed new legislation for the protection of personal data and data privacy that involve the implementation of controls that enable legal scrutiny of the mass surveillance practices that they engage in.

9.2 Bridging gaps

Given the current circumstances as described in the previous Chapters, there is still a need for the bridging of considerable policy and legal gaps. In order to better protect the two critical rights of expression and privacy, as well as the right to information and transparency in the digital age, this Report points to further actions that need to be taken, in the following aspects:

- More positive measures should be taken by national State authorities to secure the rights to privacy and freedom of expression in various forms, including by: a) encouraging the self-regulation and co-regulation of the private sector of the Internet, including provision for transparency and redress, and without pre-empting or excluding the role of independent courts to make final decisions; b) updating legal protection to adapt to new circumstances by new legislation and law interpretation; and c) improving transparency in e-governance and e-democracy developments.

- More clearly-drafted State laws are needed for the protection of privacy and freedom of expression, which reflect the shifted scopes of the conflicting rights and values. In particular, legitimate exceptions and derogations should be narrow and under procedural scrutiny that follows international human rights law and constitutional law standards, including those of legitimacy, necessity and proportionality. In the case of hate speech online, the Rabat principles can reduce potential damage to legitimate expression. The UNESCO R.O.A.M. principles are also important to consider, particularly in regard to how any balancing of rights impacts on Openness and Accessibility, and the value of multi-stakeholder participation in such balancing.

- More privacy and freedom of expression protection measures should be taken by private companies, thus recognizing their long-term interest in the protection of both rights. These measures should include transparency reports and clear privacy clauses. Internet intermediaries should be shielded from liability for third party content. Terms of service and implementation of content moderation policies should also be transparent and narrowly-defined, and opportunities for redress should be offered.

- More international and regional cooperation among national authorities is needed to enhance the protection of both rights. Such cooperation may be achieved in several ways, including by enhancing the possibility of reaching any needed international agreements on cross-border data protection, whether in the form of soft law or other alternatives.

- More efforts should be made to raise awareness and understanding through future investigations, concerning the influences of rapid ICT evolutions—e.g. those increasing the number and/or effects of privacy intrusive technologies such as IoTs, IoEs, smart devices (for use in smart homes, smart cities and smart borders), and drones—on: a) human life; b) the two fundamental rights; and c) the transparency of those technologies.

9.3 Recommendations for online privacy protection

In view of the privacy challenges analysed and discussed in the previous Chapters, this Report proposes for consideration further action in the following fields:

At the individual level, the raising of individuals' awareness should be a main focus of attention, because individuals still lack substantial understanding relating to many escalating negative impacts on their private lives – even while the same individuals make increasing use of digital devices that may impinge on their privacy, whether by "choice" or because of the many factors that render the use of such devices so useful and unavoidable. The awareness-raising activities should be extended from the understanding of the privacy impacts of existing and/or new ICTs, to sufficient knowledge, know-how and tools—such as user-friendly communication encryption tools, and online anonymity instruments—that would enable individuals to protect their own privacy.

More specifically, this may be achieved as follows:

- Governments should undertake initiatives to raise critical awareness, such as by initiating and financing special programmes/projects for this purpose. These can encompass public promotion activities, public interest advertisements on public media, including TV and radio; special TV programs; Data Privacy Day (similar to the one organized by the EU); and promotion programmes in educational institutions, and in particular through what UNESCO calls Media and Information Literacy.[622]

- Players from the private sector, in particular from ICT companies, should take substantive measures to foster privacy awareness and promote new know-now, including by providing more information to customers. As data controllers or processors, they should take more active steps to define and employ more privacy enhancing technologies (PETs) to achieve trustworthiness in their services and gain

622 http://www.unesco.org/new/en/communication-and-information/media-development/media-literacy/mil-as-composite-concept/

their consumers' trust, which will improve their reputation and eventually result in economic benefit. Like governments, players from the private sector could pass the message to individual users by reporting more about privacy breaches and harms.

- Civil society organizations play an important role too in representing their consumers in litigation, providing organizational and operational skills for collective privacy promoting activities and in presenting the individual's interests in the law and policy-making processes, bridging potential gaps left by the private sector and public bodies. They should be encouraged and supported to take additional roles in the future policy and law-making processes in Internet Governance to represent individual end users.

At the national level, multiple efforts and substantial measures could be taken at the regulatory and governance levels to improve privacy protection. Also, PETs should be encouraged and promoted as a general Internet policy, and financial arrangements should be made to support and promote technical innovation and novelty.

- Laws and policies dealing with privacy should be defined or updated to adjust to the new circumstances of the digital age, thus attaining better coverage and protection of the right to online privacy.
  - More specifically, this may be achieved by new legislation, legal amendments, and/or legal interpretations made by capable legal authorities.
  - Regulatory improvements can be made in many ways, including by: providing constitutional privacy protection; promulgating special data protection instruments, like Data Protection Laws in EU Member States and other countries; adding privacy protection clauses in new legislations like Section D of the Health Insurance Portability and Accountability Act (HIPAA); and having special online privacy protection regulations like the USA Children's Online Privacy Protection Act (COPPA).
- The protection of online anonymity plays an important role in the protection of individual privacy. Thus, it is recommended that State authorities do not mandate real name registration, unless such registration is necessary to authenticate a user for security reasons and by the user's consent.
- It is advisable to have special data protection authorities responsible for data protection and data privacy protection in the field. National Data Protection Authorities in EU Member States have made considerable contributions to the data protection and privacy protection of EU citizens, for years, with noticeable achievements. Their association Article 29, as a collective body of Data Protection Authorities, has issued authoritative opinions and statements regarding multiple issues in EU's data protection practices, which are widely respected by their national counterparts and lawyers.
- Transparency in the processing of data should be promoted and secured by each national State, insofar as this enables better privacy protection with respect to the data held by both the private and the public sector.
  - This includes steps to grant individual citizens and capable institutions by law the right to access the information regarding their data collection and processing, and to correct the data in the case of inaccuracies.

- In particular, the State should have the positive duty to disclose laws and policies regarding data privacy protection to the public, and to prescribe to private companies a duty of proper disclosure regarding data processing.

- State privacy laws should set data breach notification as mandatory for all data controllers, unless such breach would cause pressing State security and public order concerns.

- In the context of State surveillance—whether this is targeted or mass surveillance—it is suggested that transparency, from the State authority's perspective, is crucial to improving the public's trust and the Internet users' confidence in the Internet as a secure communication medium. It is recommended that State authorities make contributions in three aspects:

  - they should have clear rules and procedures that define the legal capacity of intelligence service agencies and their duties to disclose necessary information to supervising bodies—e.g. a capable court—if such disclosure to the public is not possible;

  - clear distinctions should be drawn between 'surveillance practices for law enforcement purposes' and 'intelligence services purposes';

  - while anti-terrorism is a pressing policy task in many countries, relevant surveillance measures intended to counter terrorism should not override the privacy interest of the innocent public, and should be balanced with proper procedural safeguards. For instance, when a search warrant is not possible or desirable for the sake of urgency, post hoc reporting duties might be a good option. The protection of the confidentiality of sources of journalism in the digital age could be specifically provided for, including through revised legislation where appropriate.[623]

- For State authorities, technical solutions to enhance privacy protection are an alternative or complementary measure that is efficient and effective. It is highly recommended that State policies encourage and promote the concept and practice of PbD among market players and public bodies processing personal information and data. PbD should be mandatory for public bodies and private sector players as data controllers fulfilling public functions. From the outset of their tasks, privacy concerns must be identified and mitigated early and comprehensively and PETs should be adopted and integrated.[624] It is suggested that State authorities take positive steps to promote technical instruments to better protect individual privacy, including PETs, even in the private sector.

- As a further safeguard of the right to privacy, it is recommended that State authorities take active steps to offer efficient and effective remedies to individuals via judicial, administrative, or arbitration channels. Procedural and data privacy laws should

623 UNESCO, (2015), *World Trends in Freedom of Expression and Media Development: special digital focus*. Paris: UNESCO. http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/wtr-special-digital-focus-2015/; UNESCO (2015), *Protecting Journalism Sources in the Digital Age*. Paris: UNESCO. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/images/Themes/Freedom_of_expression/safety_of_journalists/Protecting_Journalism_Sources_in_Digital_Age_UNESCO_Flye.pdf

624 Ann Cavoukian, (2009) *Privacy by Design ... Take the Challenge*, Ontario, Canada, pp. 2 and 4, available at <https://www.privacybydesign.ca/index.php/paper/pbd-book/>.

facilitate the processing of litigation that involves individuals. They could also consider a shift of duties in presenting evidence in decision-making procedure. Collective or class litigations should be allowed before a court by individual consumers when confronting a large-scale privacy breach or violation.

At the international level, there could be increased commitment by States and the rest of international society to improve privacy, even though numerous initiatives have already been taken. There should be more regional or international collaborative efforts, whether via concrete programs or mutual-agreements, to improve data protection (or data privacy) among participating States in order to regain trust in cross-border data transfer. Albeit the EU-USA Safe Harbour program failed to meet its original purposes, the principle endures as a means to encourage and secure data flow between different regions and countries, with some level of guarantee at least. Additionally, there should be more substantial moves from rhetorical principles or mere guidelines to concrete data protection measures at the international level, perhaps especially so in the case of the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Information, or the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

Fair treatment of personal data and equal privacy protection of individuals in foreign jurisdictions is an important aspect for individuals to enjoy the fundamental right to privacy as guaranteed by international human rights law. It is recommended that State authorities take active actions to respect and protect foreigners' data privacy rights in a world where cross-border data flow is so ubiquitous, and also a pre-condition for the well-functioning of the global economy and communication.

In addition, considering the mass data breach in case of cyber-attacks from criminals and unknown foreign sources, the international community should take positive actions, not only by national States but also by Internet security organizations and technical communities, to avoid such *cyber-attacks*. This kind of cyber-attacks should be prevented with all means by international cooperation of related countries to avoid further occurrence or escalation.

9.4 Recommendations for online freedom of expression protection

At the individual level, a person's exercising of the right to freedom of expression and opinion and freedom of information depends, in part, on the individual's Media and Information Literacy; e.g. competencies in Internet literacy, privacy literacy, ethical literacy and digital security. Thus, UNESCO's umbrella concept of Media and Information Literacy (MIL) should be promoted and integrated into formal and informal education systems, in recognition of the important roles that digital literacy in particular plays in promotion of the rights to freedom of expression, freedom of information, privacy, education, assocation, sustainable development, etc. Media and Information Literacy courses should be compulsory from primary education level, with the aim of teaching basic knowledge and skills that would facilitate access to the Internet and learning a variety of online communication skills, including in relation to the use of SNSs for group communication and expression. Measures should also be taken by national States to reduce the "digital divide",[625] as well as digital illiteracy, by offering assistance to disabled and elderly people, and in particular to citizens

625 Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 16 May 2011, UN Doc. A/HRC/17/27, para. 17, available at <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27>.

from developing countries with limited access possibilities, who may have difficulties relating to Internet access and/or expression in online contexts.

At the national level, since Internet access is essentially no less important than other public services—e.g. water and electricity—in daily life, competent State authorities could consider protecting individuals' *access to the Internet as a public utility, even if not a right,* as done by Finland, Estonia, and France. State authorities should find ways to reduce the costs involved in the use of broadband services—including by means of by public subsidies if needed—rendering such services affordable to every citizen.

Furthermore, to secure online freedom of expression, State authorities should establish *clear laws*, following the international standards set out by the UN capable bodies and regional human rights courts, to limit restrictions in relation with online free expression to the minimum, and to only impose such restrictions when exceptions and derogations are necessary. Among other exceptions, online defamation and online privacy invasion should be *decriminalized* in many countries, even if the relevant legal provisions are not enforced in practice. This helps avoid the use of privacy as an online censorship tool. Similarly, to avoid stifling of the right to freedom of expression and transparency, such notions as 'national security' and 'public morals' should not be interpreted too broadly, but in the light of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information [626] and the Tshwane Principles on National Security and the Right to Information[627].

Also, State authorities should enact sufficiently specific laws that define—proportionally—both the Intermediaries' legal rights and their limited liability responsibilities regarding both privacy protection and freedom of expression protection. On the one hand, State authorities should not manipulate intermediaries to restrict access to the Internet and/or control Internet contents; e.g. by asking them to arbitrarily block, filter and/or censor unwanted content, and in particular political dissent. It is recommended that more breathing space be given to intermediaries to enable the thriving of free speech in general. On the other hand, State authorities should protect individuals against and upon privacy invasion and/or violations in their right to freedom of expression, including such invasions or violations that may result from excesses linked to market competition or the actions of individuals.

For access to information or data held by public bodies and the private sector, transparency is important in imposing a positive duty on the data controllers to disclose information not merely upon requests but, in the case of public information and data that are of public interest, pro-actively, online and/or offline, by following pre-prescribed rules, whether in the hands of the private or the public sector.

In particular, the protection of the online expression of journalists and Internet (new) media producers should receive due attention, because of the role played by these actors in transparency and public life. It is also recommended that new online media and online freelance or other reporters be offered protection equating with that offered to professional journalists. Additionally, cases of defamation and privacy invasion should have higher thresholds for litigation and the granting of remedies when these actors are potential defendants.

626 Johannesburg Principles on National Security, Freedom of Expression and Access to Information https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf

627 Tshwane Principles on National Security and the Right to Information https://www.fas.org/sgp/library/tshwane.pdf

It is recommended, in order to promote the right to online free speech, for State authorities to permit additional technical means that would enable and/or enhance freedom of expression and freedom of information, including online tools that may support anonymization, such as VPNs, GUnet, Tor, and encryption-based tools that may allow individual users to communicate online without worrying about undue interception or losing personal information. It is, in particular, not recommended to fragment the Internet by controlling and separating national Internet spaces from the rest of the Internet.

At the international level, the right to freedom of expression (including press freedom and the right to information), globally, is universal. However, each national State and cultural community has its own understandings of the right. The blocking and censorship of online content in one country may also impact on the information available in other countries, across the globe. For instance, blocking activities that would have caused many DNS corruptions could affect the rest of the world.[628] For this reason, the international society is not immune to moral responsibilities to promote freedom of expression globally. It is therefore recommended for States and international organizations to support:

- More sharing of good practice in balancing freedom of expression with other rights and the role of transparency therein.
- More efforts to provide substantive support to improve freedom of information where this is an issue.
- More cooperation in addressing cross-border data protection and conflicts of jurisdiction, for instance, in the form of international or regional treaties, or improved Mutual Legal Assistance (MLA) to set out certain minimum standards for the protection of online privacy and freedom of expression.

9.5 Promoting transparency as key to balancing

Given the significance of transparency in facilitating multiple communal values, including those of privacy and freedom of expression, substantial measures could be taken to improve transparency in both private and public institutions at the national and international levels. This would be achieved by means of such constructs as transparency reports, procedural guarantees and monitoring mechanisms, accompanied by stronger protection of the citizens' right to information and the broader right to freedom of expression. Such measures and instruments should be integrated in future e-government and e-democracy systems, including during the course of their development.

Importantly, more efforts should be spent in exploring the mechanisms and instruments that may be used for the balancing of privacy, freedom of expression and transparency in the digital age, to resolve the ever-increasing and more complex conflicts that arise between them. Good balancing should always be under international human rights standards, procedural checks and made in terms of long-run public interest, as opposed to any short-term goals held by the individuals and/or parties engaging in such balancing, and therefore in the shaping of the future.

628 Thomas Fox-Brewster, "Accidental DDoS? How China's Censorship Machine Can Cause Unintended Web Blackouts", *Forbes*, 26 January 2015, available at <http://www.forbes.com/sites/thomasbrewster/2015/01/26/china-great-firewall-causing-ddos-attacks/>, accessed 11 May 2015.

9.6 Consolidated policy recommendations to key actors on privacy, free expression and transparency

Seen from the perspective of key actors, the above recommendations can be summarized as follows:

For **State actors**, consideration could be given for more efforts in:

- Updating the legal protection framework to adapt to new circumstances in the digital age by clearly-set legislation and the interpretation of law regarding the related concept and scope of the rights to privacy and freedom of expression, as well as clarifying exemptions and derogations of the two rights. In particular, legitimate exceptions and derogations should be narrowly defined and put under procedural scrutiny that follows international human rights law and constitutional law standards, including those of legitimacy, necessity and proportionality. In the case of hate speech online, the Rabat principles can reduce potential damage to legitimate expression. The UNESCO R.O.A.M. principles are also important to consider, particularly in regard to how any balancing of rights impacts on Openness and Accessibility, and the value of multi-stakeholder participation in such balancing;

- Encouraging self-regulation, within the framework of international human rights, of the private sector in areas where it does not yet seem appropriate to intervene with legislation at the national level;

- Where appropriate and possible, looking to align national law with emerging legal standards possibly through the use of legal instruments such as existing or new multinational treaties;

- Improving transparency in future e-governance and e-democracy development of public bodies, establishing parameters for the private sector carrying out public functions by clear procedural requirements and safeguards;

- Enacting new laws that restrict surveillance, by clarifying related legal duties towards users as data subjects and the boundaries in sharing data with law enforcement agencies, and providing well-defined procedural safeguards;

- Encouraging the use of encryption amongst citizens, as well as other technical means that enable anonymization, possibly with substantive means—including financial subsidies—for software and hardware development;

- Protecting online anonymity by not mandating real name registration, unless such registration is necessary to authenticate a user for security reasons and by the user's consent;

- Supporting and encouraging the ICT industry in regard to Privacy Enhancing Technologies (PET) development and standard setting for Privacy by Design (PbD) for the ICT industry;

- Stopping support to countries seeking to obtain or develop ICT technologies to infringe human rights and taking steps internationally to promote human rights, including the two discussed in this report;

- Taking active measures to improve the protection of citizens' data and privacy in case of data transfer to third countries, including by international cooperation, mutual legal assistance instruments, or other possible law instruments;

- Respecting and protect foreigners' data privacy rights in a world where cross-border data flow is so ubiquitous, and also a pre-condition for the well-functioning of the global economy and communication;

- Advocating for protection of online expression of journalists and social media producers of journalism because of the role played by these actors in transparency and public life. It is also recommended that new online media and online freelance or other reporters be offered protection equating with that offered to professional journalists. Additionally, cases of defamation and privacy invasion should have higher thresholds for litigation and the granting of remedies when these actors are potential defendants;

- Raising critical awareness among Internet users, such as by initiating and financing special programmes/projects for this purpose. These can encompass public promotion activities, public interest advertisements on public media, including TV and radio; and special TV programmes;

- Promoting relevant programmes in educational and other institutions, and in particular through what UNESCO calls Media and Information Literacy (MIL). This includes making Media and Information Literacy courses as compulsory from primary education, with the aim of teaching basic knowledge and skills that would facilitate rights on the Internet, and learning a variety of online communication skills and ethics, including in relation to the use of SNSs for group communication and expression;

- Reducing the digital divide as well as digital illiteracy, by offering assistance to disabled and elderly people, and in particular to citizens from developing countries with limited access possibilities, who may have difficulties relating to Internet access and/or expression in online contexts.

For the **private sector and Internet intermediaries**, it is recommended that consideration be given to:

- Take substantive measures to foster privacy awareness and promote new know-now, including by providing more information to customers. As data controllers or processors, they should take more active steps to define and employ more privacy enhancing technologies (PETs);

- Take more transparency measures wherever possible and appropriate, including by means of internal policies and structures, clarified privacy policies, transparency reports, and human rights impact assessments; terms of service and implementation of content moderation policies should also be transparent and narrowly-defined, and opportunities for redress should be offered;

- Follow higher standards aligned to international human rights and improve self-regulation and co-regulation with regards to the protection and promotion of privacy, transparency and freedom of expression;

- Respect the human rights of foreign citizens, including when operating on foreign territory, while following local law requirements, and unless it is unlawful to do

so, producing relevant transparency reports; promote policies whereby Internet intermediaries should be shielded from liability for third party content.

For **international society**, including UN organizations, transnational organizations and other regional organizations or institutions with international responsibilities, it is important to consider to:

- Continually emphasize the importance of the rights to privacy and free expression in the digital age;
- Foster more international and regional cooperation among national authorities to enhance the protection of both rights. Such cooperation may be achieved in several ways, including by enhancing the possibility of reaching any needed international agreements on cross-border data protection, whether in the form of soft law or other alternatives;
- Negotiate and develop international standards that deal with privacy and the protection of personal data while also trying to minimise on-line surveillance across borders;
- Foster more sharing of good practice in balancing freedom of expression with other rights and the role of transparency therein and provide substantive support to improve freedom of information where this is an issue;
- Take positive actions, along with other actors including national States, Internet security organizations and technical communities, to avoid cyber-attacks that violate freedom of expression and/or privacy. Cyber-attacks should be prevented with all means by international cooperation of related countries to avoid further occurrence or escalation;
- Improve digital literacy as a life skill within Media and Information Literacy and reduce the digital divide by providing inter alia educational measures, especially in developing countries.

For the **technical community**, it is recommended to consider to:

- Develop and promote technical solutions to enhance privacy protection as alternative or complementary measures to regulatory and self-regulatory steps. From the outset of their tasks, privacy concerns must be identified and mitigated early and comprehensively and Privacy Enhancing Technologies should be adopted and integrated;
- Promote additional technical means that would enable and/or enhance freedom of expression, including freedom of information, including online tools that may support anonymization, such as VPNs, GUnet, Tor, and encryption-based tools that may allow individual users to communicate online without worrying about undue interception or losing personal information;
- Not fragment the Internet into national intranets.

For **civil society and individual users**:

- Civil society should continue to promote the rights to privacy and freedom of expression in the digital age, empowering citizens about these rights, and monitoring violations of these rights in both the digital and non-digital realms;

- Civil society organizations play an important role too in representing their consumers in litigation, providing organizational and operational skills for collective privacy promoting activities and in presenting the individual's interests in the law and policy-making processes, bridging potential gaps left by the private sector and public bodies. They should be encouraged and supported to take additional roles in the future policy and law-making processes in Internet Governance to represent individual end users;

- Individual users should have more awareness of both rights and make efforts to improve their Media and Information Literacy; e.g. competencies in Internet literacy, privacy literacy, ethical literacy and digital security;

- Take cognisance that the two rights assessed in this Report are also considered in UNESCO's 2015 Internet Study "Keystones to foster inclusive Knowledge Societies"[629], which provides the Internet Universality concept[630] which has been endorsed by UNESCO's 195 Member States in November 2015. In terms of this concept, the reconciling of free expression and privacy rights where needed should also take account of intersections with the principles of Openness and Accessibility, as well as be undertaken in a multi-stakeholder modality. This can inform the broader process of decision making in the Internet Universality perspective.

629 http://www.unesco.org/new/en/internetstudy
630 http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/internet-universality/

Abbreviatons and acronyms

ACHR	American Convention of Human Rights
APEC	Asia-Pacific Economic Cooperation
AR	African Region
BCRs	Binding Corporate Rules
CBPR	Cross Border Privacy Rules
CCTV	Closed Circuit Television
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women
CoE	Council of Europe
COPPA	Children's Online Privacy Protection Act
CRC	Convention on the Rights of the Child – or – Committee on the Rights of the Child
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DPA	Data Protection Authority
DPD	Data Protection Directive
DPI	Deep Package Inspection
EaaS	Everything as a Service
ECJ	European Court of Justice
ECOWAS	Economic Community West African States
ECtHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security
EU	European Union
FISA	Foreign Intelligence Surveillance Act
FOI	Freedom of Information
FTC	Federal Trade Commission
GC	General Comment
GFW	Great Firewall
GNI	Global Network Initiative
GPS	Geographical Positioning System
HIPPA	Health Insurance Portability and Accountability
HRC	Human Rights Committee
IaaS	Infrastructure as a Service
IAB	Internet Architecture Board
IACHR	Inter-American Commission on Human Rights
ICAAN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant of Civil and Political Rights
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination
ICESCR	International Covenant of Cultural, Economic and Social Rights
ICTs	Information Communication Technologies
IETF	Internet Engineering Task Force
IG	Internet Governance
INGOs	International Non-governmental Organizations
IoP	Internet of People

IoT	Internet of Things
IP	Internet Protocol
ISPs	Internet Service Providers
IT	Information Technology
ITU	International Telecommunication Union
IXP	Internet Exchange Point
LEAs	Law Enforcement Agencies
LGBTI	Lesbian, Gay, Bisexual, Transgender and Intersex
LSAs	Intelligence Service Agencies
MLAT	Mutual Legal Assistance Treaty
NGOs	Non-governmental Organizations
NSA	National Security Agency
OAS	Organization of American States
OECD	Organization for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
OPA	Online Privacy Alliances
PaaS	Platform as a Service
PbD	Privacy by Design
PC	Personal Computer
PETs	Privacy-Enhancing Technologies
PHI	Protected Health Information
PII	Personable Identifiable Information
PITs	Privacy-Invading Technologies
PNRs	Passenger Name Records
RFID	Radio-Frequency Identification
RTI	Right to Information
RUDs	Reservations, understandings, and declarations
SARS	Severe Acute Respiratory Syndrome
SIS	Secret Intelligence Services
SMEs	Small and Medium-sized Enterprises
SNP	Social Network Platform
SNS	Social Networking Services
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UPN	User Principal Name
U.S.A.	United States of America
VPNs	Virtual Private Networks
WGIG	Working Group Internet Governance
WSIS	World Summit on Information Society

Appendix 1: UNESCO Connecting the Dots Outcome Document

United Nations Educational, Scientific and Cultural Organization

CONNECTING THE DOTS: OPTIONS FOR FUTURE ACTION

Outcome document

The "CONNECTing the Dots: Options for Future Action" Conference held at UNESCO Headquarters 3-4 March 2015,

Noted the potential of the Internet to advance human progress towards inclusive Knowledge Societies, and the important role of UNESCO in fostering this development within the wider ecosystem of actors,

Affirmed the human rights principles that underpin UNESCO's approach to Internet-related issues, specifically that the same rights that people have offline must be protected online as per Human Rights Council resolution A/HRC/RES/26/13;

Recalled Resolution 52 of the 37th session of the General Conference, which mandated a consultative multi-stakeholder study with options for consideration of Member States, to be reported to the 38th General Conference within the framework of UNESCO's work on the World Summit on the Information Society,

Further recalled the establishment of principles in guiding documents that include the article 12 and 19 of the Universal Declaration of Human Rights, and article 17 and 19 in the International Covenant on Civil and Political Rights;

And, having *reviewed* the draft of the UNESCO consultative study,

Commend continued work on the related options below, and look forward to UNESCO Member States deliberations on them:

1. Overarching options for UNESCO

    1.1 Considering the Final Statement of the first WSIS+10 conference, endorsed by the 37th General Conference, affirm the on-going value of the World Summit on the Information Society (WSIS) outcomes, including the Internet Governance Forum (IGF), for the post-2015 development agenda, Internet governance issues, and the role and work of UNESCO;

    1.2 Affirm that the fundamental human rights to freedom of opinion and expression, and its corollary of press freedom and the right of access to information, and the right to peaceful assembly, and the right to privacy, are enablers of the post-2015 development agenda;

    1.3 Also affirm that increasing access to information and knowledge across society, assisted by the availability of information and communication

technologies (ICTs), supports sustainable development and improves people's lives;

1.4 Promote the alignment of Internet-related laws, policies and protocols with international human rights law;

1.5 Support the Internet Universality principles (R.O.A.M) that promote a Human Rights-based, Open Internet is Accessible to all and characterized by Multi-stakeholder participation;

1.6 Strengthen the cross-cutting role of the Internet in all of UNESCO programmatic activities, including Priority Africa, Priority Gender Equality, support to Small Islands Developing States and Least Developed Countries, as well as in UNESCO's leadership of the International Decade for the Rapprochement of Cultures.

2. Options for UNESCO related to the field of Access to Information and Knowledge:

2.1 Foster universal, open, affordable and unfettered access to information and knowledge, and narrowing the digital divide, including the gender gap, and encourage open standards, raise awareness and monitor progress;

2.2 Advocate for ICT policies that enhance access guided by governance principles that ensure openness, transparency, accountability, multilingualism, inclusiveness, gender equality, and civil participation including for youth, persons with disabilities, marginalized and vulnerable groups;

2.3 Support innovative approaches to facilitate citizen involvement in the development, implementation and monitoring of the Sustainable Development Goals, as agreed at the UN General Assembly;

2.4 Promote universal access to information and knowledge and ICTs by encouraging the creation of public access facilities, and by supporting users of all types to develop their capabilities to use the Internet as creators and users of information and knowledge;

2.5 Reaffirm the important contribution provided by open access to scholarly, scientific and journalistic information, open government data, and free and open source software, towards the building of open knowledge resources;

2.6 Explore the potential of the Internet for cultural diversity.

3. Options for UNESCO related to the field of Freedom of Expression

3.1 Urge Member States and other actors to protect, promote and implement international human rights law on free expression and the free flow of information and ideas on the Internet;

3.2 Reaffirm that freedom of expression applies, and should be respected, online and offline in accordance with Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) that any limitation on freedom of information must comply with international human rights law as outlined by Article 19(3) of the International Covenant on Civil and Political Rights;

3.3 Support safety for journalists, media workers, and social media producers who generate a significant amount of journalism, and reaffirm the importance of the rule of law to combat impunity in cases of attacks on freedom of expression and journalism on or off the Internet;

3.4 Noting the relevance to the Internet and digital communications of the international Convention on the Rights of Persons with Disabilities (CRPD), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and the work of the Office of the High Commissioner on Human Rights, concerning the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (Rabat Plan of Action 2012), promote educational and social mechanisms for combating online hate speech, without using this to restrict freedom of expression;

3.5 Continue dialogue on the important role that Internet intermediaries have in promoting and protecting freedom of expression;

4. Options for UNESCO related to Privacy

4.1 Support research to assess the impacts on privacy of digital interception, collection, storage and use of data, as well as other emerging trends;

4.2 Reaffirm that the right to privacy applies and should be respected online and offline in accordance with Article 12 of the UDHR and Article 17 of the ICCPR and support as relevant within UNESCO's mandate, the efforts related to UN General Assembly Resolution A/RES/69/166 on the Right to Privacy in the Digital Age;

4.3 Support best practices and efforts made by Member States and other stakeholders to address security and privacy concerns on the Internet in accordance with their international human rights obligations and consider in this respect the key role played by actors in the private sector;

4.4 Recognise the role that anonymity and encryption can play as enablers of privacy protection and freedom of expression, and facilitate dialogue on these issues.

4.5 Share best practices in approaches to collecting personal information that is legitimate, necessary and proportionate, and that minimizes personal identifiers in data;

4.6 Support initiatives that promote peoples' awareness of the right to privacy online and the understanding of the evolving ways in which governments and commercial enterprises collect, use, store and share information, as well as the ways in which digital security tools can be used to protect users' privacy rights;

4.7 Support efforts to protect personal data which provide users with security, respect for their rights, and redress mechanisms, and which strengthen trust in new digital services.

5. Options for UNESCO related to Ethical dimension of the Information Society

   5.1 Promote human rights-based ethical reflection, research and public dialogue on the implications of new and emerging technologies and their potential societal impacts;

   5.2 Incorporate, as a core component in educational content and resources, including life-long learning programmes, that support the understanding and practice of human rights-based ethical reflection and its role in both online and offline life;

   5.3 Enable girls and women take full advantage of the potential of the Internet for gender equality through taking proactive measures to remove barriers, both online and offline, and promoting their equal participation;

   5.4 Support policy makers in enhancing their capacity to address the human right-based ethical aspects of inclusive knowledge societies by providing relevant training and resources;

   5.5 In recognition of the trans-boundary nature of the Internet, promote global citizenship education, regional and international cooperation, capacity-building, research, the exchange of best practices and development of a broad understanding and capabilities to respond to its ethical challenges.

6. Options for UNESCO related to cross-cutting issues:

   6.1 Promote the integration of UNESCO's expertise on Media and Information Literacy (MIL) into formal and informal education systems, in recognition of the important roles that digital literacy and facilitating universal access to information on the Internet, play in the promotion of the right to education, as enumerated in Human Rights Council, Resolution 26/13;

   6.2 Recognize the need for enhanced protection of the confidentiality of sources of journalism in the digital age;

   6.3 Support Member States as requested in the harmonization of relevant domestic laws, policies and practices with international human rights law;

   6.4 Support transparency and public participation in the development and implementation of policies and practices amongst all actors in the information society.

   6.5 Promote research into law, policy, regulatory frameworks and the use of the Internet, including relevant indicators in the key areas of the study.

   6.6 Promote UNESCO's participation in discussions on Network Neutrality as relevant to the fields of access to information and knowledge and freedom of expression.

7. Options related to UNESCO role

   7.1 Reinforce UNESCO's contributions and leadership within the UN system, including continued implementation of the WSIS outcomes, the WSIS+10 review, the IGF and the post-2015 development agenda;

7.2 Engage as relevant with partners outside of the UN system, such as individual governments, civil society, news media, academia, private sector, technical community and individual users; including by providing expert advice, sharing of experience, creating fora for dialogue, and fostering development and empowerment of users to develop their capacities;

7.3 Support Member States in ensuring that Internet policy and regulation involves the participation of all stakeholders, and integrates international human rights and gender equality.

Appendix 2: UNESCO Concept paper on Internet Universality

Internet Universality: A Means Towards Building Knowledge Societies and the Post-2015 Sustainable Development Agenda

2 September 2013

Abstract

UNESCO's Communication and Information Sector is canvassing a new concept of "Internet Universality", which could serve to highlight, holistically, the continued conditions for progress towards the Knowledge Society and the elaboration of the Post-2015 Sustainable Development Agenda. The concept includes, but also goes beyond, universal access to the Internet, mobile and ICTs. The word "Universality" points to four fundamental norms that have been embodied in the broad evolution of the Internet to date, and which provide a comprehensive way to understand how multiple different aspects are part of a wider whole. For the Internet to fulfill its historic potential, it needs to achieve fully-fledged "Universality" based upon the strength and interdependence of the following: (i) the norm that the Internet is Human Rights-based (which in this paper is the substantive meaning of a "free Internet"), (ii) the norm that it is "Open", (iii) the norm that highlights "Accessible to All", and (iv) the norm that it is nurtured by Multi-takeholder Participation. The four norms can be summarized by the mnemonic R – O – A – M (Rights, Openness, Accessibility, Multi-stakeholder). The "Internet Universality" concept has very specific value for UNESCO in particular. By building on UNESCO's existing positions on the Internet, the concept of "Internet Universality" can help frame much of UNESCO's Internet-related work in Education, Culture, Natural and Social Sciences and Communication-Information for the strategic period of 2014-2021. As regards global debates on Internet governance, the "Internet Universality" concept can help UNESCO facilitate international multi-stakeholder cooperation, and it can also help to highlight what the Organization can bring to the Post-2015 Sustainable Development Agenda.

By: Division of Freedom of Expression and Media Development

Communication and Information Sector[631]

* An integral version of this paper in all UN offcial languages is online at:

http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/internet-universality/

631 Incorporating insights from UNESCO Inter-sectoral and external consultations. We also thank Ms Constance Bommelaer for her contribution to the development of the concept.

Summary version (4 pages)

1. Why a concept of "Internet Universality"?

UNESCO has long recognized that the Internet has enormous potential to bring the world closer to peace, sustainable development and the eradication of poverty.[632] As an international intergovernmental organization that operates with a global remit and promotes values that are universal, UNESCO has a logical connection to the Internet's "universality". This "universality" can be understood as the common thread that runs through four key social dimensions pertaining to the Internet, namely the extent to which this facility is based on universal norms of being: (i) Human Rights-based (and therefore free); (ii) Open; (iii) Accessible to All; and (iv) Multi-stakeholder Participation. The four norms can be summarized by the mnemonic R – O – A – M (Rights, Openness, Accessibility, Multi-stakeholder).

Various stakeholders have characterized the Internet according to what they perceive as its essential features, highlighting one or other aspects such as freedom of expression, open architecture, security issues, online ethics, etc.[633] What this range of conceptualisations illustrates is both the diversity of concerns and interests, as well as the multi-faceted character of the Internet itself. In turn, this prompts the question as to the possibility of understanding how the various considerations and dimensions relate to each other and to the wider whole. As a method to conceptualize this bigger picture, UNESCO is now canvassing the concept of "Internet Universality", which could serve as a macro-concept. The purpose is to capture the enduring essentials of the vast, complex and evolving Internet, and which facilitates a comprehensive understanding of where and how different parties, and especially UNESCO, relate to the Internet. The concept could particularly serve as an enabling perspective in the context of the increasing centrality of Internet to societies, and specifically the increasing "Internetization" of education, the sciences, culture and communication-information.

As well as identifying four distinctive norms that have special interest to UNESCO, the concept of "Internet Universality" groups these under a single integrated heading in a way that affords recognition of their mutually reinforcing and interdependent character. Without such a comprehensive intellectual device, it would otherwise be hard to grasp interconnections amongst UNESCO's Internet-related work and how it contributes to Knowledge Societies and the Post-2015 Sustainable Development Agenda.

As regards UNESCO's involvement in global debates, the concept of "Internet Universality" can be considered for its potential as a unifying, consolidated and comprehensive framework. On the one hand, it highlights the freedom and human rights principles as shared by those existing notions such as "Internet freedom"; on the other hand, it also

632 For example: "Reflection and Analysis by UNESCO on the Internet: UNESCO and the use of Internet in its domains of competence" (2011). http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ED/ICT/pdf/useinternetdomains.pdf.

633 For example, there have been different emphases at the Stockholm Forum, the Freedom Online Coalition on Cyberspace, Wilton Park, and the London and Budapest conferences on Cyberspace. Similarly, the Internet has been analyzed diversely by international organisations. Examples here are: the Council of Europe's "Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet" (2011), the OECD Council Recommendation on Principles for Internet Policy Making (2011), the OSCE Representative on Freedom of the Media Recommendations from the Internet 2013 Conference (2013); the ICC Policy Statement on "The freedom of expression and the free flow of information on the Internet", and the Internet Rights and Principles Coalition's "Internet Rights & Principles Charter" (2010).

provides an umbrella to address the intertwined issues of access and use, as well as the matters of technical and economic openness. In addition, the concept also encompasses multi-stakeholder engagement as an integral component. In this inclusive way, the "Internet Universality" concept can therefore be a bridging and foresighted framework for dialogue between North and South and among different stakeholders. As such, it could also make a unique contribution to shaping global Internet governance discourse and the post-2015 Sustainable Development Agenda.

2. Unpacking the concept of "Internet Universality"

The linking of four normative components of the "universality" of the Internet builds closely upon prior UNESCO thinking about the Internet which includes:

- *Recommendation on the Promotion and Use of Multilingualism and Universal Access to Cyberspace* (2003).[634] (This document particularly points to the accessibility norm, as well as the need to balance rights).
- *Reflection and Analysis by UNESCO on the Internet* (2011).[635] (This document highlights normative work in relation to UNESCO's programmes, and multi-stakeholder participation).
- *Final Recommendations of WSIS+10 review event*, and the *Final Statement of the WSIS+10 review event* (2013).[636] (These cover rights, access, openness, and multi-stakeholder issues).
- *UNGIS (UN Group on the Information Society) Joint Statement on the Post-2015 Sustainable Development Agenda* (2013).[637] (This document highlights the importance of the social conditions for Information and Communication Technologies in general, and the Internet in particular, to contribute to inclusive Knowledge Societies).

"Internet Universality" integrates a range of existing UNESCO insights and shows the link between the Internet and what UNESCO has already recognised[638] as the underlying key principles of Knowledge Societies: freedom of expression, quality education for all, universal access to information and knowledge, and respect for cultural and linguistic diversity. In this way, the concept highlights what is needed for the Internet to be a means towards achieving Knowledge Societies. It serves as a heuristic to highlight that the Internet's character and utility entail technical, social, legal, economic and other arrangements which in turn depend on particular norms that underpin the positive potentiality of this facility. Considered in more depth, the R – O – A – M norms constitutive of "Internet Universality" (Rights, Openness, Accessibility, Multi-stakeholder) can be understood as follows:

634 http://www.unesco.org/new/en/communication-and-information/about-us/how-we-work/strategy-and-programme/promotion-and-use-of-multilingualism-and-universal-access-to-cyberspace/.

635 http://unesdoc.unesco.org/images/0019/001920/192096e.pdf;

636 Documents from the First WSIS+10 Review Event, "Towards Knowledge Societies for Peace and Sustainable Development", Paris 25-27 February, 2013: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_recommendations_en.pdf; http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf

637 http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/ungis_joint_statement_wsis_2013.pdf.

638 *Reflection and Analysis by UNESCO on the Internet,* http://unesdoc.unesco.org/.images/0019/001920/192096e.pdf.

(i) By identifying the Internet's connection to Human Rights-based norms as constituents of freedom, "Internet Universality" helps to emphasize continued harmony between the growth and use of the Internet and human rights. A free Internet in this sense means one that respects and enables the freedom to exercise human rights.[639] In this regard, "Internet Universality" enjoins us to consider the gamut of interdependencies and inter-relationships between different human rights and the Internet – such as freedom of expression, privacy, cultural participation, gender equality, association, security, education, etc.

(ii) "Internet Universality" also highlights the norm of the Internet being Open. This designation recognizes the importance of technological issues such as open standards, as well as standards of open access to knowledge and information. Openness also signals the importance of ease of entry of actors and the absence of closure that might otherwise be imposed through monopolies.

(iii) Accessible to All as a norm for "Internet Universality" raises issues of technical access and availability, as well as digital divides such as based on economic income and urban-rural inequalities. Thus it points to the importance of norms around universal access to minimum levels of connectivity infrastructure. At the same time, "accessibility" requires engaging with social exclusions from the Internet based on factors such as literacy, language, class, gender, and disability. Further, understanding that people access the Internet as producers of content, code and applications, and not just as consumers of information and services, the issue of user competencies is part of the accessibility dimension of "Universality". This highlights UNESCO's notion of Media and Information Literacy which enhances accessibility by empowering Internet users to engage critically, competently and ethically.

(iv) The Internet in this sense cannot only be seen from the "supply side", but needs a complimentary "user-centric" perspective. The Participatory, and specifically the Multi-stakeholder engagement, dimension of "Internet Universality" facilitates sense-making of the roles that different agents (representing different sectors as well as different social and economic status, and not excluding women and girls) have played, and need to continue to play, in developing and governing the Internet on a range of levels. Participation is essential to the value that the facility can have for peace, sustainable development and poverty eradication. In bridging contesting stakeholder interests, participative mechanisms contribute to shared norms that mitigate abuses of the Internet. "Universality" here highlights shared governance of the Internet.

These norms for these four aspects are distinct, but they also reinforce each other. Rights without accessibility would be limited to the few; accessibility without rights would stunt the potential of access. Openness allows for sharing and innovation, and it complements respect for rights and accessibility. Multi-stakeholder participation helps guarantee the other three norms. Overall, an Internet that falls short of respecting human rights, openness, accessibility or multi-stakeholder participation would by definition be far less than universal.

639 In this manner, "Internet Universality" accords with the Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and also echoes the first resolution on "promotion, protection and enjoyment of human rights on the Internet" passed by UN Human Rights Council in 2012.

3. How the concept of "Internet Universality" is relevant to UNESCO

UNESCO has a unique role in promoting "Internet Universality". It is the UN agency with a mandate that spans social life at large and, within this, has programs that involve the Internet in education, culture, science, social sciences and communication-information. By using "Internet Universality" as an umbrella concept, UNESCO can position more specific concerns such as mobile learning, education for girls, cultural and linguistic diversity, media and information literacy, research into climate change, freedom of expression, universal access to information, bioethics and social inclusion, etc. In this way, "Internet Universality" can also support the priorities of Gender Equality and Africa. It can serve as an over-arching, integrating framework for Internet-related work across UNESCO, establishing a common frame of reference for all. Operationally the concept can elevate a range of work to the status of initiatives that jointly advance "Internet Universality". It can encourage synergies and inter-sectoral co-operation and joint programming. In particular, the concept can enhance understanding of the mid-term strategy of 2014-2021 (37/C4) and the quadrennial program (37/C5).

4. Conclusion

"Internet Universality" accords with the Organization's service to the wider international community in the following respects:

- Laboratory of ideas, including foresight – elaborating the concept is directly relevant to UNESCO's creative and think-tank potential;
- By stimulating global debate, "Internet Universality" illustrates how UNESCO can be a catalyst for international cooperation, with a holistic and inclusive approach.
- Standard-setter – if the concept gained traction broadly, it could inform the development of standards for monitoring progress in "Internet Universality"
- As a normative framework that can inform policies, and draw in public and private, civil society and decision-makers, "Internet Universality" can help UNESCO fulfill its role as a capacity-builder in Member States.

Looking ahead, "Internet Universality" could follow in the footsteps of previous influential intellectual work by UNESCO such as the concepts of "Intangible cultural heritage" and "Knowledge Societies". Because "Internet Universality" represents an updated conceptualization of the era, the concept could become a valuable contribution to the global discussion about this complex and dynamic human creation and serve to enhance Internet's continued contribution to humanity's shared future.

Privacy, free expression and transparency

It is widely agreed that human rights should apply as much online as offline, and that freedom of expression and privacy should be no exception. But there are particular complexities in the online environment.

This publication explores these issues in the context of UNESCO's new approach to Internet issues. The approach was adopted by our 195 Member States in November 2015, and is based on the Outcome Document of an earlier conference called CONNECTing the Dots.

Concretely, this means that UNESCO stands for the concept of "Internet Universality" and the related "ROAM principles" which refer to a Human-rights-based, Open and Accessible Internet that is governed by Multi-stakeholder participation.

It is in this context that the current study was commissioned to address very specific rights and associated values.

In the digital age, the challenge is to see how tensions between rights operate in relation to the Internet, and therefore in relation to the ROAM principles.

The purpose of the current research was precisely to unpack some of these issues. In particular, it probes the complex interplay on the Internet between the right to freedom of expression (and information), transparency, and the right to privacy. The research explores the boundaries of these rights, and the various modalities of reconciling and aligning them.

The study analyses the legal framework, current mechanisms for balancing rights, and specific issues, cases and trends. As revealed by the research, traditional laws and regulations for the protection of privacy and freedom of expression often do not deal with digital issues.

Also covered are the interplay and interactions between multiple players – e.g. the State agents, Internet users, ICT companies, civil society organizations, the judiciary and the security services. Various policy recommendations are made that address both key issues and various stakeholders groups.

United Nations
Educational, Scientific and
Cultural Organization

Communication and
Information Sector

9 789231 001888